CITY UNIVERSITY
LONDON

Examining the Influence of Safety Management in the Personal Spaceflight Industry

Charles Andrew Quinn

Submitted for the degree of Doctor of Philosophy in Air Safety Management at City University London, School of Engineering and Mathematical Sciences

January 2012

Andy Quinn

PhD in Air Safety Management

City University London
School of Engineering and Mathematical Sciences
Energy and Transport Centre
Aeronautics and Air Transport Group

Thesis

Examining the Influence of Safety Management in the Personal Spaceflight Industry

---

Supervisors:

Supervisor: Dr Steve Bond

External: Professor Paul Maropoulos (University of Bath)

I certify that this project is wholly my own work and that all material extracted from other sources is clearly referenced.

This thesis contains 100,284 words in total, less Appendices, using the Microsoft Word Windows 7 word count command.

For my wife;

For her patience, her understanding and her love

Abstract

Suborbital flights will soon take flight as a viable commercial operation. Operators such as Virgin Galactic, along with their designer Scaled Composites, will be responsible for safety of the flight crew, Spaceflight Participants and indeed the uninvolved public beneath their flight trajectories.

Within the United States, the Federal Aviation Authority's Office of Commercial Transportation (FAA-AST) has provided Launch License Regulations and Guidelines for prospective design organisations and operators alike. The aim of this thesis is to analyse suborbital spaceflight approaches to safety management and to determine whether effective safety management is being or could be applied to influence vehicle design and subsequent operation.

The thesis provides a review of current safety-related information on suborbital spaceflight, existing space safety information and also existing aviation safety information. The findings of the review concern two main areas; firstly that a gap exists within suborbital safety management criteria, and secondly that a gap exists in existing aviation-based safety guidelines.

In the first case, the research concluded that FAA-AST safety management criteria did not present sufficiently explicit and rationalised guidelines for this new industry. Indeed, the thesis argues that the scope of the FAA-AST regulations (covering both orbital and suborbital aspects) is too broad, and that regulations and guidelines should be split into distinct orbital and suborbital sections so as to provide more effective directives.

In Europe, no such regulations or guidelines exist as there has until now been no requirement (a 'customer') for the European Aviation Safety Agency (EASA) to implement such a framework. This thesis sought to address this gap by using a safety tool (Goal Structuring Notation) to construct a goal-based regulatory approach, which was included in a draft EASA suborbital Policy.

Secondly, the main significant finding of this research is that a gap (literally) exists between current aviation-based design organisation safety guidelines and operator safety risk management guidelines. This absence of communication means operators are not managing their safety risks as effectively as they could. The thesis argues that the suborbital domain should take heed, as most vehicles are based on aircraft designs and therefore suborbital operators will, no doubt, apply 'best practice' either from the aviation or commercial space domains. Neither is appropriate or effective.

As a result of the main finding a contiguous safety model has been developed which employs a 'key (platform) hazard' to join the design organisation analysis to the operator safety risk management, therefore completing an explicit sequence from the initiating causal event to the accident. The model is demonstrated using case studies from space disasters (Space Shuttle) and also from aviation accidents (Air France flight AF447); the model details the explicit accident sequence and shows missing or failed controls leading up to the accident.

The research enabled models to be constructed and also proposed additional and explicit guidelines for the suborbital industry such as medical and training standards and separate safety criteria for vertical launch vehicles; these are included as recommendations and need to be ratified by recognised bodies such as the International Association for the Advancement of Space Safety's Suborbital Space Safety Technical Committee for inclusion in their Space Safety Standards Manual. In the latter case these recommendations are already agenda items for the Technical Committee to address.

Acknowledgements

I would like to thank my City University supervisor Dr Steve Bond whose guidance and enthusiasm for the like-minded Eureka moments has inspired me. Additionally I would like to thank my external supervisor from Bath University Professor Paul Maropoulos in particular for his sturdy hand in re-structuring the approach during the early days.

I would also like to thank those at EASA for their persistence in getting a research framework going and in particular Jean-Bruno Marciacq for having faith and also for his professionalism and support over the years.

From industry I would like to thank Jose Mariano Lopez Urdiales and Jose Miguel Bermudez Miquel from zero2infintiy for allowing me to analyse the safety management aspects of their near-space balloon project - 'BLOON'.

Another stalwart colleague whom deserves acknowledgment is Clive Lee who has provided constructive guidance on papers and in general and also for his brilliant mathematical mind. We have agonised over safety criteria in normal work-day tasks and we too had our Eureka moments. This questioning of apparent best practice has helped me examine those existing aviation and space-related frameworks more closely.

Finally I would like to thank my eldest son Chris whom has used his extensive talents to bring my safety model to life in the form a web-based hazard log. I provided the requirements from my knowledge of hazard logs and he used his creative skills to form the basis of a useful tool; this now needs to be developed further by a software company to become a marketable safety product. Additionally Chris's skills gained from his work as an editorial assistant in a publishing house has been most valuable in helping to correctly set out the format of the Thesis – muchas gracias Chris.

Table of Contents

CHAPTER ONE – Introduction & Research Strategy

1. INTRODUCTION

This Thesis is purposely focused on the Personal Spaceflight Industry and therefore concentrates on the nascent suborbital domain. It is recognised that fee-paying individuals have been to the International Space Station by means of a Soyuz rocket and are deemed fully fledged astronauts; these people have been assigned a scientific project to enable them to be eligible. They have also been trained under the government-based requirements and have launched under government-based existing regulations and guidelines and so this part of the 'personal spaceflight' is not included as part of the research.

In October 2006 it may have appeared late in terms of trying to influence policy and guidelines with Virgin Galactic planning flights in 2007/2008; however no suborbital flights have taken place over the period of the research and a realistic start to suborbital operations is more likely to be in 2012/2013. Additionally no design or operating activities have taken place in Europe and the European Aviation Safety Agency (EASA) was not tasked with producing regulations for suborbital aircraft operations. Thus the opportunity still existed for the activities of the research to influence decision-makers in their regulations and guidelines and possibly to influence operators.

1.1. RESEARCH AIMS

1.1.1 TO ANALYSE THE SUBORBITAL SPACEFLIGHT APPROACHES TO SAFETY MANAGEMENT

Personal Spaceflight is an emerging field and the initial approach to ensure safety has been driven from the FAA through the Commercial Space Launch Amendments Act of 2004 (CSLAA) and with the Federal Aviation Administration Office of Commercial Space Transportation (FAA-AST) as adjudicators. The Advisory Circulars (AC), Notice of Proposed Rulemaking (NPRM) and Code of Federal Regulations (CFRs) detail the activities required for:

- Safety Engineering
- Safety Management
- Basic Training
- Flight Crew
- Participants – with waivers to say that they understand the risks and that the vehicle is not certified

Is this sufficient? Are participant waivers appropriate? Within Europe and under EASA remit, the FAA guidelines and regulation are probably not appropriate.

This thesis examines the delta between the FAA approach to Safety Management, including Spaceflight Training & Medical requirements and a possible European approach. The research aims to examine the Safety Management 'best practices' in the aviation and space domains in order to determine if a suitable 'Safety Model' exists for the emerging industry

1.1.2 TO ASSIST IN DEVELOPING SAFETY MANAGEMENT METHODOLOGY FOR SUBORBITAL SPACEFLIGHT

Based on the analysis of the identified approaches to suborbital spaceflight there is an opportunity to assist in developing appropriate methodology in the safety activity and training fields.

Another aim of the research is to use the analysis and determine the gaps that exist and to identify new and integrated methods in approaching safety.

1.1.3 TO ASSIST IN THE SETTING OF SAFETY & TRAINING STANDARDS FOR SUBORBITAL SPACEFLIGHT

As the commercial spaceflight is immature and the FAA guidelines are extremely flexible, there is an opportunity to assist in setting the regulatory standards for safety in Europe, including medical and training standards. An aim of the thesis is to influence safety standards and training/medical standards in the emerging field.

1.1.4 TO IDENTIFY POSSIBLE TECHNOLOGICAL RESOLUTIONS FOR SPACEFLIGHT OPERATORS BASED ON CURRENT & EMERGING TECHNOLOGIES

When analysing the leading operator's spacecraft designs, it is clear that in some areas there are weaknesses in their methodology and safety has not been an influential factor – rather it has been a solution-based methodology as opposed to a full acquisition cycle with safety input along the way.

Therefore, this part of the research aims to identify emerging technologies and examines whether retrospective application is possible using safety analysis techniques.

1.2. **RESEARCH OBJECTIVES**

1.2.1 GAP ANALYSIS

A gap analysis is the first objective in order to determine the shortfalls in the suborbital spaceflight approach in comparison to the aviation and governmental space programmes. The gap analysis will be applied to the following areas:

- Safety Management Systems
- Safety Criteria
- Hazard Management
- Risk Management
- Training
- Medical
- Emerging Technologies

1.2.2 SPACEFLIGHT SAFETY ACTIVITIES

One of the objectives is to undertake safety activities should a gap be identified during the analysis; the following are anticipated 'gaps' from the initial research, networking and conferences attended:

- European Suborbital Aircraft Safety Criteria
- Safety Management System for Spaceports
- Safety Assessment of Operator – although it was hoped that 'Rocketplane' or Virgin Galactic would have provided an opportunity for analysis this did not materialise. Instead the company Zero2Infinity were content for a safety analysis to be conducted regarding their 'near space' BLOON project.
- A contiguous safety model

1.2.3 SPACEFLIGHT MEDICAL & TRAINING ACTIVITIES

Another objective is to review and then analyse the extremely limited medical and training guidelines suggested by the FAA. The objectives of this part of the research is related to the actual medical criterion and training that is derived from synthesised safety analysis i.e. training that is required as mitigation to specific Hazards.

1.2.4 IDENTIFICATION & REVIEW OF EMERGING TECHNOLOGY APPLICATIONS FOR SPECIFIC USE BY INDUSTRY

The final objective is to identify emerging technologies and to review these for their suitability for the commercial spaceflight industry; one method used is a safety technique – Cost Benefit Analysis. This is used as part of the 'As Low As Reasonably Practicable' (ALARP) process. It is anticipated that this may be qualitative rather than quantitative due to the immaturity of the industry however this part of the research will examine (by synthesised safety analysis) the additional technology-based risk reduction measures as part of an ALARP Evaluation process.

1.3. RESEARCH FRAMEWORK OUTPUTS

Research framework agreements have been sought with relevant organisations in order to undertake the research activities. The purpose of the agreements is to be able to provide safety influence in achieving stated objectives; an example with the European Aviation Safety Agency (EASA) is to provide safety rules and guidelines for the European Suborbital Aircraft (SoA) Industry. The framework agreements were finalised during the academic year 2010-2011. The research was then able to continue with the author being involved in the Preliminary Regulatory Impact Assessment; however the European Commission (EC) has not yet approved the task for EASA and therefore the task is only part complete. Nonetheless the research thus far has enabled a partial summary of the SoA Policy to be produced and also has enabled the author to continue with a more in-depth analysis which is presented as 'supplemental considerations' to the Policy; the aim here is that EASA can elect to include parts of the supplemental research as part of their guidelines whereas the Policy will be kept at a high level.

The following areas were hoped to be covered and the thesis goals had to remain flexible over the period of the research due to prospective opportunities not materialising:

- EUROPEAN SAFETY CRITERIA – EASA task started and currently on hold; research continued and has provided 'supplemental considerations' for EASA as well as a SoA Policy goal-based safety argument structure
- SPACEFLIGHT TRAINING PROGRAMME– not materialised and this is instead covered in Chapter 3
- SAFETY MANAGEMENT SYSTEM – SPACEPORT– not materialised and a synthesis has been conducted in Chapter 4
- SAFETY MANAGEMENT SYSTEM FOR OPERATOR – the author provided safety guidance for Virgin Galactic (SMS framework) however the contract required a Non-Disclosure Agreement and therefore the work could not be included in the thesis
- EMERGING TECHNOLOGY REVIEW – 'zero2infinity' – Non Disclosure Agreement in place to research the safety criteria and emerging technologies for the 'Near-Space' Balloon experience (BLOON). This has been completed in Chapter 4.

1.4. METHOD OF RESEARCH

1.4.1 RESEARCH FRAMEWORK METHODOLOGY

The research methodology employed is captured in Figure 2 below using a Goal Structuring Notation (GSN) approach. GSN is a graphical representation of an argument and is the preferred methodology for articulating a safety case; this application of the technique is discussed further in Chapter 2.2. The GSN is used here to represent the research undertaken and is used to argue the completeness and effectiveness of the thesis; as such it was used as a 'living' document throughout the life of the research and updates have occurred as a result of changing situations; an example was that

'Rocketplane' were the designated Spacecraft Operator for analysis under formal Non-Disclosure Agreement, however due to financial issues they are no longer developing a commercial spacecraft[1]. Also Virgin Galactic work could not be reproduced due to Non-Disclosure Agreements. This has led to another Operator being sought for analysis and Zero2Infinity were content for their BLOON project to be analysed within a research framework during the later stages of the thesis. Additionally the European Aviation Safety Agency (EASA) research framework took longer than expected and eventually started in January 2011; this was subsequently placed 'on hold' in May whilst the European Commission made their decision on the Preliminary Regulatory Impact Assessment.

GSN Symbols:

The following GSN graphical notation is used both in the research methodology 'Thesis Case' and also for a proposed 'future-state' EASA goal-based regulatory safety case in Chapter 3.

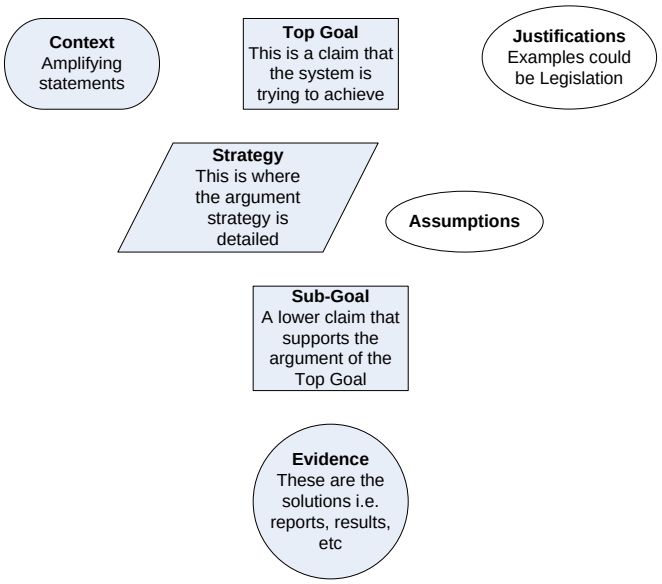


Figure 1: Goal Structuring Notation graphical 'nodes'

The 'Thesis Case' Top Goal has amplifying statements (Context) such as definitions, the aims and objectives of the research. The Top Goal is supported by an argument (Top Strategy) detailing the sub-goals; Review (Goal 1), Gap Analysis (G2), proposed safety models and guidelines for a 'future-state' (G3) and an effective validation process (G4). The argument is then supported by evidence that the research has been completed and validated (solutions E.1.1 etc.).

[1] Rocketplane have since resurfaced in April 2011 and are linked with possible opportunities in Holland with the 'Spacelinq' project.

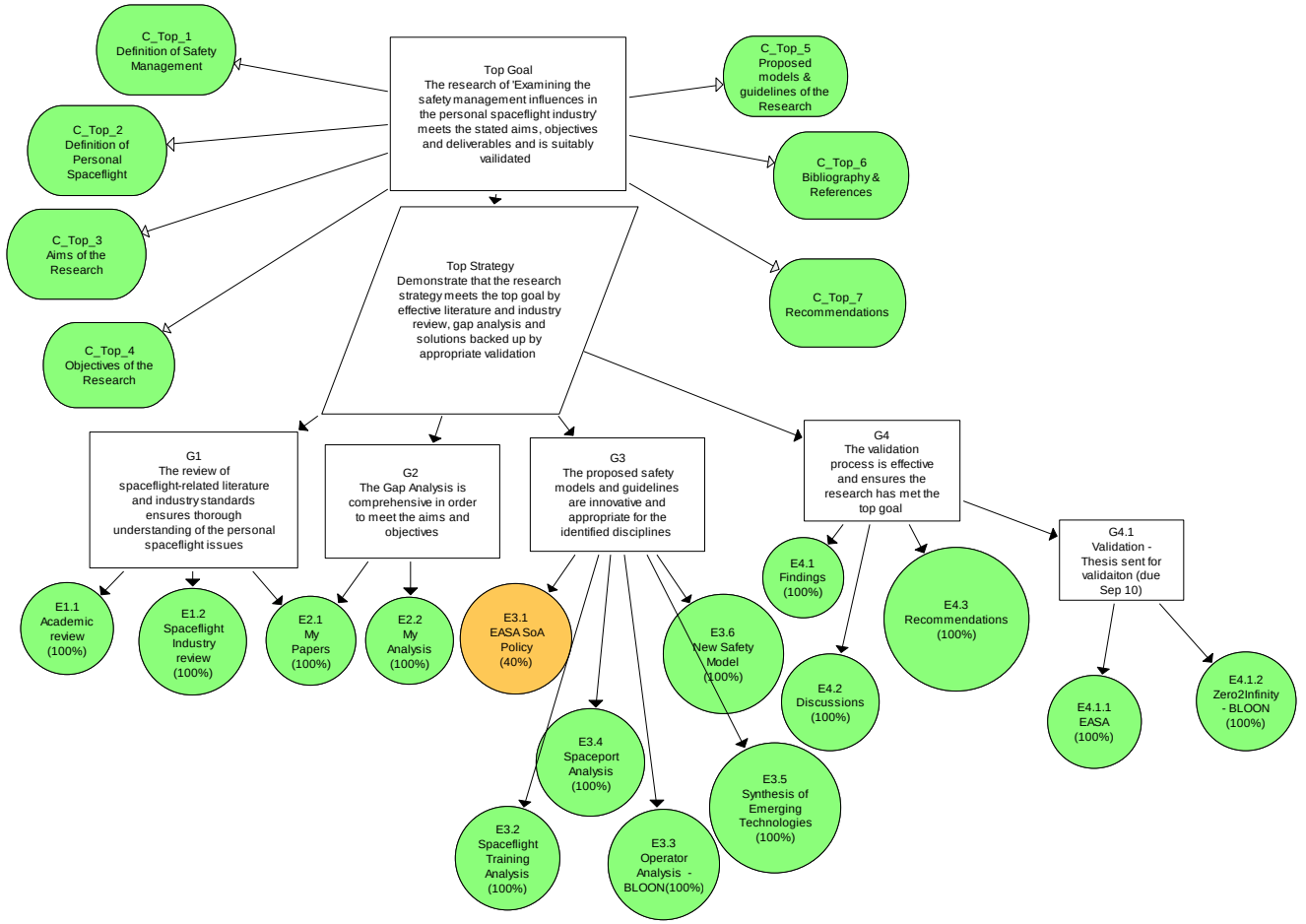


Figure 2: Research Methodology and Results using Goal Structuring Notation – unable to complete task E3.1 due EASA resourcing

1.4.1.1 'THESIS CASE' FRAMEWORK

- Top Goal: The research of 'Examining the Influence of Safety Management in the Personal Spaceflight Industry' meets the stated aims, objectives and deliverables in order to satisfy the criteria for the award of PhD.

The Context of which the 'Top Goal' is argued is as follows:

- Context 1 [C_Top_1]: Definition of Safety Management; A Safety Management System is a safety organizational function concerned with implementing and managing safety policies and procedures necessary to undertake formal safety risk management (see Section 2.2).
- C_Top_2: Definition of Personal Spaceflight; for the purpose of this Thesis, Personal Spaceflight is considered as travel to space by fee-paying personnel [space is further defined as 100km, see Section 1.7].
- C_Top_3: Aims of the Research (See Section 1.1)
- C_Top_4: Objectives of the Research (See Section 1.2)
- C_Top_5: Proposed models and guidelines of the Research; these are those documents (results of particular research) produced as part of a research framework with an organising body, such as the SoA Policy and guidelines for EASA and also the safety analysis for Zero-2-Infinity. Also the *SATURN SAFETY MODEL* and resultant hazard log will be a product of the research and it is intended that this will be peer reviewed.
- C_Top_6: Bibliography & References (see bibliography & references as appropriate)
- C_Top_7: Recommendation from the Research in terms of Safety & Training & 'other' aspects considered (see Section 6.3)

The **Top Goal** is supported by a logical research strategy (**Top Strategy**) which demonstrates that the research meets the top goal. This Top Strategy is supported by four strands of the argument; an effective review (Goal **G1)**, a Gap Analysis (**G2**), innovative proposed models, guidelines and methodologies (**G3**) and validation of the research (**G4**):

- (G1): The review of spaceflight-related literature and industry standards ensures thorough understanding of personal spaceflight issues; G1 is supported by Evidence of sufficient literature review (E1.1) and Evidence of Personal Spaceflight Industry review (E1.2).
- (G2): The Gap Analysis is comprehensive in order to meet the aims and objectives; G2 is supported by Evidence (E2.1) Authors Papers and Evidence (E2.2) Authors Gap Analysis.
- (G3): The proposed models, guidelines and methodologies are innovative and appropriate for the identified disciplines; G3 is supported by Evidence (E3.1) EASA Policy[2] (E3.2) Spaceflight Medical & Training Analysis, (E3.3) Operator Analysis (E3.4) Spaceport Analysis, (E3.5) Synthesis of Emerging Technologies and (E3.6) New Safety Model.
- (G4): The validation process is effective in ensuring the Thesis has met the Top Goal; G4 is supported by Evidence (E4.1) Authors Findings, Evidence (E4.2) Authors Discussions and also Validation by Industry Evidence and G4.1 is supported by Evidence (E4.1.1) EASA validation, (E4.1.2) Operator validation and (E4.1.4) External Supervisor validation.

[2] The EASA evidence (E3.1) is shown 40% complete because the task for the next phase has not been authorised for EASA by the EC. The 40% claim is due to the initial Pre-RIA being complete and the author's efforts in the EASA Policy Safety Case and Supplemental Considerations as detailed in Chapter 3.

The evidence that the goals have been met is justified at section 5.6.

1.5. **REVIEW OF LITERATURE AND RELEVANT SAFETY TECHNIQUES**

The review phase of the research concentrates on the spaceflight domain but also examines the safety techniques from the aviation domain.

1.5.1 LITERATURE REVIEW

Personal Spaceflight is an emerging field with the FAA-AST leading the way; hence the literature review strategy is twofold:

- Review of FAA-AST Rules and Guidelines for the Industry. This involves reviewing initial FAA-AST documents and then reviewing updates to them as they are issued; an example of this is the AC No.437.55-1 [18] which has superseded the previous 2005 version (AC No.431.35-2A). The reviews are captured in Chapter 2.1.
- Review of Books, Journals and articles on spaceflight; this includes information on government-led space programmes, such as National Aerospace & Space Agency (NASA), European Space Agency (ESA) documents and other relevant space standards. These reviews are also captured in Chapter 2.1.

1.5.2 EMERGING PERSONAL SPACEFLIGHT INDUSTRY REVIEW

Although the Personal Spaceflight Industry is yet to begin commercial operations, there has been increased interest during the last few years and the progress of companies such as Virgin Galactic has been slow but notable. This part of the review covers relevant papers from space-related conferences and also covers relevant articles from the emerging Industry (Chapter 2.1.2).

1.5.3 GAP ANALYSIS

A GAP Analysis is defined in the 'Business Directory' as:

> *'Technique for determining the steps to be taken in moving from a current state to a desired future-state'*

In terms of the gap analysis undertaken in Chapter 2.3.2 the purpose is to analyse the current state in regards to the applicable Safety Management activities relating to the FAA's Rules and Guidelines and other applicable standards. The rationale is that the first Personal Spaceflight launches will be undertaken in America and the FAA-AST are the only governing body to have published criteria for designers and operators to follow. The outcome of the gap analysis can be viewed as one step in moving from the current state and Chapter 3 examines a possible policy and guidelines for EASA consideration in moving forward to a desired future-state.

1.5.4 REVIEW OF SAFETY 'TOOLS'

It is necessary to review the different approaches to Safety Management and System Safety in order to determine which aspects are applicable and considered 'best practice' such that they can be taken forward to the emerging Personal Spaceflight Industry. The reviews are captured in Chapter 2.2.

1.5.5 REVIEW OF SPACEFLIGHT MEDICAL STANDARDS

Understanding the principles of Safety Management and in particular Risk Management will enable a clear understanding of what hazards are present and what mitigation strategies are required. Having a robust medical strategy will form important mitigation to minimise the likelihood of harm to the spaceflight participants. Chapter 2.3.4 examines the FAA regulations (current state).

1.5.6 REVIEW OF TRAINING APPROACHES

A component of a Safety Management System (SMS) is 'Training' and a review of the different approaches of how to establish training for the Personal Spaceflight Industry is necessary because of the complex and demanding environment that spaceflight passengers or 'participants' (SFPs) will be subjected to. The reviews are captured in Chapter 2.3.6; these include a comparison of governmental (NASA), military and civilian training approaches as well as the FAA regulations (current state).

1.5.7 SAFETY INFLUENCE

The main purpose of the research is to examine whether safety management can influence the emerging Personal Spaceflight Industry. The methodology for determining Safety Influence hinges on the results of the gap analysis in Chapter 2.3.2 and then examines whether the policies, guidelines and models presented by the 'gaps' can be effectively applied to the areas discussed in Chapter 3 and hence influencing a move from the current state to a future-state. This is achieved through research frameworks with organisations as detailed in 3.2 and 4.4; where research frameworks are not available then the 'guidelines' will be validated accordingly.

1.5.8 SYNTHESIS

Chapter 4 presents a synthesis of emerging and current technologies that may have a direct impact on the safety of the vehicle and people on board. This chapter also examines the benefit of utilising one of the identified technologies against the cost of implementing the technology (for instance as a control measure); one of the safety techniques involved is 'Cost Benefit Analysis' which is reviewed in Chapter 2.2 in the first instance.

1.6. **RESEARCH ASSUMPTIONS & PRE-REQUISITES**

1.6.1 ASSUMPTIONS:

It is assumed that the models and guidelines from this research are treated in accordance with standard Intellectual Proprietary rules.

1.6.2 PRE-REQUISITES:

It is a pre-requisite that the personnel contacted for information about their 'spaceflight-related' company or for validation of this research are Suitably Qualified Experienced Personnel (SQEP).

1.7. **THESIS ROADMAP FOR THE READER**

The thesis starts with an introduction to space tourism because there are already orbital fee paying 'astronauts' who fly on the existing governmental program on board a Russian Soyuz spacecraft. This thesis however concentrates on the nascent suborbital domain and the introduction therefore describes the origins of the X-Prize in 2004 to commercial development in 2011.

Having set the scene for the suborbital 'space' industry Chapter 2 then reviews the relevant information available. As the suborbital industry is yet to take off it was important to reflect on the current orbital spaceflight accidents to gauge the safety of the space industry. Next a review of existing safety tools and techniques was carried out to determine how this was achieved and whether this could be improved for the suborbital domain. Here it was also considered necessary to review the aviation-based safety guidelines because most suborbital vehicles have aircraft-like designs. Finally within Chapter 2 a review of existing commercial spaceflight legislation and guidelines was carried out along with other emerging and related guidelines.

Chapter 3 details possible ways in which Safety Management can influence the emerging industry by addressing the key gaps identified in Chapter 2. In the first instance the recommendations from this

thesis have been transferred to the Suborbital Safety Technical Committee of the International Association for the Advancement of Space Safety (the author is the Chair of this Technical Committee). Secondly a framework was established with the European Aviation Safety Agency (EASA) to assist in providing a Suborbital Aircraft (SoA) Policy; here the research and gap analysis provided the initial roadmap for the Policy and provided 'supplemental guidelines for consideration'. However the European Commission have stopped the work on SoA Policy due to other higher priorities within EASA and hence this meant the task was not concluded; this is detailed as further work. Additionally in Chapter 3 an exemplar safety model was developed because of the gap identified within the aviation domain; the model is relevant to the suborbital and aviation domains and case studies have been used to show how a contiguous safety management approach could prevent accidents. Chapter 3 also provides analysis of Spaceport Safety and guidelines for reducing operator risks with medical, training and protective equipment strategies.

Chapter 4 provides a synthesis of emerging technologies relevant to the suborbital domain including spacesuits, emergency systems and rocket propulsion systems. Additionally a framework was agreed with a space tourism company (Zero2Infinity) to analyse their 'near space' balloon project using the safety model and supplemental guidelines for consideration from Chapter 3.

Chapter 5 details the findings and significance of the research and provides validation of the thesis by EASA and Zero2Infinity.

Chapter 6 details the conclusions and recommendations. Additional supporting information is contained within the Appendices including a Functional Hazard Analysis, Case Studies of Space Shuttle disasters and the Air France AF447 accident and the EASA SoA Policy Goal Structuring Notation (not finished).

1.8. BACKGROUND – SPACE TOURISM

1.8.1 A NEW ERA IN SPACE TRAVEL

Travelling into Space for tourism may seem to some as fanciful and futuristic however this is already a reality courtesy of Space Adventures. There have been seven fee-paying Space Tourists thus far and more will follow; indeed Space Adventures are planning 'trips' around the Moon and back to Earth as one of their services. The first 'tourist' Denis Tito launched into Space in 2001 and Charles Simonyi liked his first experience in 2007 so much that he went to Space for a second time in 2009 (thus making it eight space tourist trips[3]).

Of course to achieve this, the Space Tourists must actually become scientific-based members of the crew embarking to spend 10 days on the International Space Station (ISS). First of all they must undergo full astronaut medical tests and training for six months and they are then classified as astronauts and are no longer considered 'Space Tourists'. Nonetheless they have paid circa $20Million for the experience and are thus still fee-paying members of the public.

Suborbital flight could be considered as the gateway to orbital flights in that commercialising space to the mass market requires a cheaper and quicker process than the existing orbital space tourism market. A suborbital flight is one that reaches an altitude higher than 100 km (62 miles, or 328,000 ft.) above sea level; this altitude, known as the Kármán line, was chosen by the Fédération Aéronautique Internationale[4]. Once the suborbital market is mature (and by implication, safe) and the costs reduced then Design Organisations (DO) and Operators will be able to derive the necessary orbital-capable machine based on the 'low cost' model for their suborbital machines.

1.8.2 THE X-PRIZE AND OTHER KEY INITIATIVES

Two dates will remain key moments in the new and exciting field of Space Tourism – 29th September and 4th October 2004, when Space Ship One (SS1) achieved heights of 103km and a record breaking 112km respectively. The flight was a 2-stage launch profile: the first stage was up to 50,000ft with the SS1 attached to a 'Mother-Ship' (the White Knight) to save on fuel; the second stage was the release of SS1 at 50,000ft, followed by rocket ignition taking SS1 to the pre-requisite 'space height' of 100km at three times the speed of sound. The spacecraft spent five minutes in the space environment under its own momentum and then returned through the atmosphere under gravity using a unique wing feathering system before returning to normal configuration and gliding back to the departure runway.

The flight of SS1 evolved from the $10M Ansari X-Prize competition [1] instigated by Peter Diamandis. The aim was to design and build a craft capable of achieving a manned 100km 'space' flight twice within a week. The objective of the prize was to demonstrate that the craft were actually 'reusable' i.e. a Re-Launch Vehicle (RLV). For this achievement to be taken forward, the Ansari X-Prize winners must evolve from a competition into a viable commercial operation. Scaled Composite's SS1 design was the baseline vehicle for Virgin Galactic's requirements to take space tourists into suborbital flight. Now seven years later Scaled Composites have designed and built Space Ship 2 and White Knight 2 and are presently in the test phase. However along the way there have been set-backs; in 2007 during a simple test of their new hybrid rocket propulsion system (nitrous oxide injector test) there was a catastrophic accident killing three scientists and injuring several

[3] http://www.spaceadventures.com/index.cfm?fuseaction=orbital.Clients
[4] See Wikipedia information on the FAI and general information on spaceflight; http://en.wikipedia.org/wiki/Federation_Aronautique_Internationale

others. This sad event should have been avoided and one could question whether a Safety Management System was in place. Scaled Composites have since moved on with the design and are looking forward to commercial operations with Virgin Galactic in the coming years.

The current X-Prize competition (Google Lunar X Prize) has a $50M prize for the team who can design and build a craft as a 'Lunar Lander' with vertical take-off and landing capabilities.

Other initiatives include Bigelow Aerospace [2] and his 'Space Hotels'; this incredible initiative's design, build and test phase is already mirroring the spacecraft's path with the idea that Operators and their designers will want to have a spacecraft that is capable of 'docking' with a space hotel. Bigelow has made impressive progress and has already launched his first two prototypes 'Genesis I' and 'Genesis II' into orbit; tests are being conducted as to the strength and rigidity of the structures currently orbiting the Earth.

1.8.3 THE SPACE MARKET

The Space market can really be split into two fields; orbital and suborbital. In the orbital field, Space Exploration Technologies (Space-X) are the leaders having won a lucrative contract from NASA to provide a commercial crew transportation system to the ISS. They have developed the Falcon-9 launch system for their Dragon spacecraft and on 8th December 2010 they became the first commercial company in history to re-enter a spacecraft from orbit; this was their first successful orbital test launch – the company experienced test launch accidents with their Falcon-9 rocket during earlier test phases (see Chapter 2).

In terms of the suborbital field, Virgin Galactic (air-launched system) is demonstrably the early leaders[5] with XCOR progressing well with a different vehicle approach (rocket-powered aircraft taking off horizontally by its own means). Other companies employing a vertical capsule system such as Armadillo Aerospace and Blue Origin are also progressing well. There are quite a few other companies in various stages of early design stages and these will emerge to fruition over the next decade.

In regards to the suborbital market projections, the updated Futron/Zogby report [3] suggests that up to 13,000 people per year could be undertaking suborbital flights by 2021. In a more recent contrasting study by the European Space Research and Technology Centre [4] the number is estimated at 15,000 people per year; the report suggests that the industry could move towards a classical aeronautical business model as soon as there would be a sufficient number of spacecraft manufacturers to cater for demand. The report further suggests that the 'luxury travel market' represents a unique chance for space tourism to get off the ground and reach the critical mass that will enable a significant ticket price decrease.

1.8.4 COMMERCIALISING SPACE

A commercial operation of this type can only be considered viable if it is also safe. Herein lays the challenge for the nascent space tourism industry. Safety is paramount, as in conventional commercial aviation; however, the risks in suborbital flights will be far greater due to the spaceflight environmental aspects. Commercial space tourism sits in the grey area between NASA and the regulated FAA-AST. This uncharted area therefore requires new regulations and standards. To give the industry impetus, it clearly requires a 2-way dialogue between the regulator and the operator of the

[5] Virgin Galactic/Scaled Composites are currently (2011) in the 'Test and Evaluation' phase; their latest successful airdrop was conducted on 4 May 2011

Reusable Launch Vehicle (RLV)/Suborbital Aircraft (SoA). This will ensure safety and also the required flexibility (in the form of disclaimers and insurances). Having an impractical and an unyielding approach would be too restrictive for the general public if they are to become space participants

The FAA has appointed the Office of Commercial Space Transportation (FAA-AST) [5] as the governing body and the CLSAA (2004) as legislation for the fledgling commercial spaceflight industry. Other commercial avenues are being examined by NASA in providing contracts to commercial companies such as 'Space-X' to provide an orbital spacecraft to re-supply the International Space Station (ISS). This contracting approach has also been extended to include Boeing and Armadillo Aerospace.

1.8.5 SAFETY, SAFETY, SAFETY

Commercial (Personal) Spaceflight is still in its infancy and regarding Safety Management policies, the FAA-AST is concentrating more on the designer's experiment permits and safety activities rather than the policies and procedures of operators; however they use the term 'operator' for Scaled Composites (for example) as the design company who will be designing, building and testing the spaceship as part of an experimental license i.e. they are not discussing Virgin Galactic as the operator.

Furthermore the FAA-AST Advisory Circular (AC) regarding Hazard Analysis is not as robust as it could be and this element is analysed during the research as part of the gap analysis in Chapter 2.3. In terms of a prospective spaceflight operator's safety management, the FAA-AST has a 3-pronged strategy towards safety assurance for RLV mission and vehicle operation's licensing. The strategy is depicted in various FAA-AST documents, including their guide to RLV Reliability Analysis [6] whereby the three strands are:

- *Using a logical, disciplined system safety process to identify hazards and to mitigate or eliminate risk,*
- *Establishing limitations of acceptable public risk as determined through a calculation of the individual and collective risk, including the expected number of casualties (Ec)*
- *Imposing mandatory and derived operating requirements*

This 3-pronged strategy is also discussed as part of the gap analysis in Chapter 2.3.

Why do we need to consider operators at such an early stage? The answer is involvement; even though an operator may not be planning to 'fly' for a number of years until the spacecraft has been designed, built and tested, the operator should have a Safety Management System in order to build a safety culture; indeed within Europe this should be mandated as part of an Air Operator Certificate (AOC) – the FAA-AST has not mandated this as yet though its aviation safety counterpart (FAA-AVS) is introducing this. Additionally as the reliability of these new spacecraft will be relatively low and essentially un-proven the operator procedural mitigation will play a large factor in providing safety assurance to the regulators; hence it is important to establish these operator procedures in conjunction with the operator.

Having a top-down and bottom-up safety effort right from the concept stage would provide tangible evidence in support of the safety effort which could avert an accident/mishap. Dianne Vaughan [7] discovered a lack of safety culture as part of the contributory aspects of the Challenger disaster at NASA:

> *'flying with ''acceptable risks'' was normative in NASA culture. The five-step decision sequence I found that characterized work group decision-making about the SRB (Solid Rocket Boosters) joints was nothing less than the working group conforming to NASA's procedures for hazard analysis….in fact the listing and description of the ''acceptable risks'' on the Space Shuttle prior to the first launch in April 1981 filled six volumes.'*

In essence, safety is a key component to the success of the evolving industry and the safety effort needs to be robust and practicable in all industry fields during the formative years. A safety culture takes time to evolve and the process should be started at the beginning of a project and be a '*just and learning'* culture. Safety Culture is discussed in Section 2.2.9.

1.8.6 EMERGING SPACE SAFETY GOVERNING BODIES AND ASSOCIATIONS

As a new domain emerges there is a requirement to govern the field in terms of legality and safety. The suborbital domain provides challenging issues such as the cross-over from 'air law' to 'space law' and sovereignty of that 'space' segment. These issues need to be addressed at various levels such as the United Nations and the International Civil Aviation Organization (ICAO) as a top priority due to the imminent start of operations from Virgin Galactic and XCOR.

There are various Associations and Federations that can provide a body of experts from within a particular field and debate and influence the way forward on challenging aspects. In terms of space safety the following are considered leading bodies (the relevant sub-committees are listed):

- International Association for the Advancement of Space Safety (IAASS)
  - Suborbital Space Safety Technical Committee (SSS TC) – this is a newly formed TC proposed and implemented by the author and discussed more in Chapter 3.
- International Space Safety Federation (ISSF)
  - Commercial Human Space Safety Committee

1.9. DEFINITIONS

The following definitions apply to this Thesis:

Term	Meaning	Source
1st Party Personnel	Individuals directly involved in operating the re-usable launch and re-entry vehicle/suborbital aircraft i.e. the flight crew/pilots	Author derived See 3.3.1
2nd Party Personnel	individuals directly involved in supporting the spacecraft/suborbital aircraft (i.e. maintainers) and individuals participating in the flight who are not members of the flight crew i.e. passengers (spaceflight participants)	Author derived
3rd Party Personnel	the uninvolved public and other uninvolved personnel within the vicinity of the spacecraft/suborbital aircraft i.e. near the vehicle on the ground such as within the boundaries of the Spaceport	Author derived
Acceptably Safe	The Risk to a suborbital aircraft has been demonstrated to have been reduced so far as is reasonably practicable and that relevant prescriptive safety targets and safety requirements have been met for all phases of the suborbital flight	Author derived See 2.2.6
Accident	An unplanned event or series of events that results in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.	AC120-92
Crew	Any employee of a licensee or transferee, or of a contractor or subcontractor of a licensee or transferee, who performs activities in the course of that employment directly relating to the launch, re-entry, or other operation of or in a launch vehicle or re-entry vehicle that carries human beings.	FAA-AST
Failure Condition	A condition having an effect on either the airplane or its occupants, or both, either direct or consequential which is caused or contributed to by one or more failures or errors considering flight phase and relevant adverse operational or environmental conditions or external events	AC23.1309
Flight crew	Any employee of a licensee or transferee, or of a contractor or subcontractor of a licensee or transferee, who is on board a launch or re-entry vehicle and performs activities in the course of that employment directly relating to the launch, re-entry, or other operation of the launch vehicle or re-entry vehicle	FAA-AST
Flight Safety System	Destructive or non-destructive system designed to limit or restrict the hazards to public health and safety and the safety of property presented by a launch vehicle or re-entry vehicle while in flight by initiating and accomplishing a controlled ending to vehicle flight	FAA-AST
Flight Termination System	Explosive or other disabling or thrust-terminating equipment installed in a launch vehicle, plus any associated ground equipment, for terminating the flight of a malfunctioning vehicle or stage	ISO-14620
'g' (in relation to G-Force)	The ratio of actual acceleration to that of the earth's gravity 'g' of 9.8m/s²	Wikipedia
Hazard	A physical situation, *condition*, or state of a system, often following from some initiating event, that *unless mitigated* may lead to an accident	Based on UK Defence Standard 00-56
Human Factors	The systematic application of relevant information about human capabilities, limitations, characteristics, behaviours and motivation to the design of systems.	UK Defence Standard 00-56
Human Rating	A human-rated system is one that accommodates human needs, effectively utilizes human capabilities, controls hazards and manages safety risk associated with human spaceflight, and provides to the maximum extent practical, the capability to safely recover the crew from hazardous situations	NASA

Independent Safety Auditor (ISA)	An individual or team, from an independent organisation, that undertakes audits and other assessment activities to provide assurance that safety activities comply with planned arrangements, are implemented effectively and are suitable to achieve objectives; and whether related outputs are correct, valid and fit for purpose	UK Defence Standard 00-56
Mishap	Unsuccessful mission due to an accident or incident	FAA-AST
RLV	A Re-Launch Vehicle (RLV) is a spacecraft designed to enter space, then re-enter and land such that the vehicle can be launched again	FAA-AST
RLV Pilot	A designated member of the RLV flight crew who has the ability to exercise flight control authority over a launch or re-entry vehicle	FAA-AST
Safe	Risk has been demonstrated to have been reduced to a level that is ALARP and broadly acceptable, or tolerable, and relevant prescriptive safety requirements have been met, for a system in a given application in a given operating environment	UK Defence Standard 00-56
Safety Case	A structured argument supported by a body of evidence that provides a compelling, comprehensive and valid case that a system is safe for a given application in a given environment	UK Defence Standard 00-56
Safety Management	The systematic management of the risks associated with operations, related ground operations and aircraft engineering or maintenance activities to achieve high levels of safety performance	UK CAA
Safety Management System	A safety organizational function concerned with implementing and managing safety policies and procedures necessary to undertake formal safety risk management	Author derived See 2.2
'Safing'	An action or sequence of actions necessary to place systems, Sub-systems or component parts into predetermined safe conditions	ISSB – Space Safety Standards
Space	Space shall be defined as the environment above the Earth, beginning at 62 miles (100km).	Fédération Aéronautique Internationale
Space flight participant (SFP)	An individual, who is not crew, carried within a launch vehicle or re-entry vehicle	FAA-AST
Suborbital rocket	A vehicle, rocket-propelled in whole or in part, intended for flight on a suborbital trajectory, and the thrust of which is greater than its lift for the majority of the rocket-powered portion of its ascent	FAA-AST
Suborbital trajectory	The intentional flight path of a launch vehicle, re-entry vehicle, or any portion thereof, whose vacuum instantaneous impact point does not leave the surface of the Earth	FAA-AST
Tolerable	A level of risk between broadly acceptable and unacceptable that may be tolerated *by society* when it has been demonstrated to be ALARP	Based on UK Defence Standard 00-56

Table 1: Definitions applicable to the Dissertation

CHAPTER TWO - Academic & Industry Review

2. INTRODUCTION

Chapter Two includes a review of academic and industry literature in the suborbital field and due to the immaturity of the Personal Spaceflight Industry this also includes reviewing relevant NASA spaceflight aspects such as lessons identified from accidents. To balance the Industry perspective, reviews of academic papers and conference presentations give an insight into various aspects on how the industry is tackling novel issues regarding Personal Spaceflight; this includes the initial European Aviation Safety Agency (EASA) standpoint on managing suborbital aircraft within a European regulatory framework. Finally, a review of aerospace safety management system tools and techniques is undertaken in order to assess their applicability to the new field.

2.1. ACADEMIC REVIEW

Suborbital space tourism has yet to take-off and already there are concerns[6] over the newcomers to the space industry. These concerns come from the safety experts within an established governmental-based space industry; the question is 'why'? To understand these concerns we must first examine all of the evidence presented by the emerging suborbital players ranging from the FAA-AST rules and guidelines, to academic papers and in particular to review those areas where we can identify 'Lessons Learned' from accidents so that we can try and avoid accidents in the suborbital domain; indeed many believe that more than one disaster in the early developmental and commercial phase could see the end of suborbital space tourism before it has the chance to mature. Let us not forget that orbital space tourism has thus far proven to be successful (and safe); this may be due to using the current launch systems (the Soyuz rocket) and with the fee-paying astronaut undergoing standard astronaut training (mitigation) and having rigid supervision (more mitigation).

2.1.1 Human Spaceflight & Aerospace Accidents

Spaceflight accidents tend to draw the attention of the media because most accidents and incidents involving rockets tend to be spectacular in the outcome (or consequences). When this involves human spaceflight, the interest level is world-wide and any disaster has severe consequences. In 50 years of spaceflight there have only been 4 'disasters' (see Table 2 below) during the 'flight' phase of the spaceflight; however there have been many more accidents and incidents resulting in deaths or injuries to astronauts and support personnel. Of these accidents, the most documented are the Space Shuttle disasters. Within these disasters 'active and 'latent' failures play a major part in the contributions to the accidents (as per most accidents) and this was clearly evident, and detailed, in the Space Shuttle 'Challenger' Board of Inquiry findings and also by Diane Vaughan.

2.1.1.1 Space Shuttle Challenger Accident

Diane Vaughan [7] cited poor managerial decision-making in the Space Shuttle 'Challenger' disaster in 1986. The Space Shuttle launched on Tuesday 28th January 1986 at 1138 Eastern Time with temperatures at 36 °F (2.2 °C)[7]; this was 15 degrees Fahrenheit lower than any previous Space Shuttle Launch. The design temperature limitations for the Solid Rocket Booster's O-ring seals were 53 °F (12 °C). National Administration Space Agency (NASA) management decided to launch against the

[6] Comment by the President of the International Association for the Advancement of Space Safety during the Space Tourism Safety Panel discussion, 20 May 2010, Huntsville, Alabama, USA
[7] http://www.spaceline.org/challenger.html

advice of the engineers and so must be seen as a major contributor to the accident. The 'Rogers Commission' cited the following regarding the root cause and also the contributory aspects of the accident:

> *'The loss of the Space Shuttle Challenger was caused by a failure in the joint between the two lower segments of the right Solid Rocket Motor. The specific failure was the destruction of the seals that are intended to prevent hot gases from leaking through the joint during the propellant burn of the rocket motor'*

> *'The decision to launch the Challenger was flawed. Those who made that decision were unaware of the recent history of problems concerning the O-rings and the joint and were unaware of the initial written recommendation of the contractor advising against the launch at temperatures below 53 degrees Fahrenheit and the continuing opposition of the engineers at Thiokol after the management reversed its position. They did not have a clear understanding of Rockwell's concern that it was not safe to launch because of ice on the pad. If the decision-makers had known all of the facts, it is highly unlikely that they would have decided to launch 51-L on January 28, 1986'.*

Here it is clear that a technical issue was compounded by an organisational (managerial) safety culture issue and this aspect is discussed more in 2.2.8 (human-machine integration), 2.2.9 (safety culture) and further analysed as part of a case study in Chapter 3.4.7.

2.1.1.2 Space Shuttle Columbia Accident

Nearly 20 years later, NASA was still making fundamental safety errors in their managerial decision-making. The Space Shuttle 'Columbia' was lost on 1 February 2003 as a result of a breach in the thermal protection system on the leading edge of the left wing; the origins of the causal factor actually happened during launch when a piece of insulating foam broke off and damaged the wing. The 'Columbia' Accident Investigation Board's report [8] also cited the poor safety culture at NASA:

> *"The organisational causes of this accident are rooted in the Space Shuttle's history and culture, including the original compromises that were required to gain approval for the Shuttle program, subsequent years of resource constraints, fluctuating priorities, schedule pressures, mischaracterisations of the Shuttle as operational rather than developmental, and lack of an agreed national vision. Cultural traits and organisational practices detrimental to safety and reliability were allowed to develop, including: reliance on past success as a substitute for sound engineering practices (such as testing to understand why systems were not performing in accordance with requirements/specifications); organisational barriers which prevented effective communication of critical safety information and stifled professional differences of opinion; lack of integrated management across the program"*

More specifically the Board found 14 other instances where the Thermal Protection System had suffered damage either from launch or from space debris and hence:

> *'Space Shuttle Program personnel knew that the monitoring of tile damage was inadequate and that clear trends could be more readily identified if monitoring was improved, but no such improvements were made.'*

It appears that little had improved in terms of proactive safety management and that the cultural issues identified from 'Challenger' were still prevalent.

2.1.1.3 UK MoD Nimrod XV230 Accident

In the UK, Charles Haddon-Cave QC was tasked with reviewing the Royal Air Force Nimrod aircraft Board of Inquiry results and his report [9] reflected on the similarities between the organisational failures of NASA to that of the UK Ministry of Defence (MoD) and Suppliers. The report concludes the accident was '*avoidable*' and that '*there has been a yawning gap between the appearance and reality of safety'* and that there were '*manifold shortcomings in the UK military -airworthiness and in-service support* regimes'.

As depicted in Haddon-Cave's report, there were many 'Active & Latent Failures' in the Nimrod accident sequence:

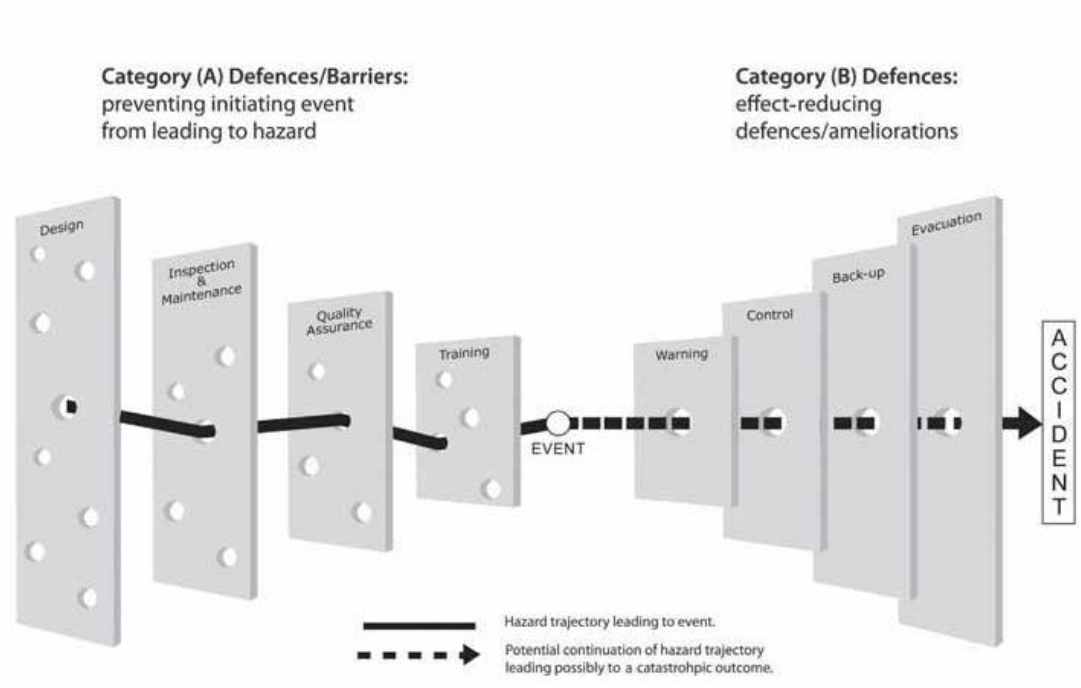


Figure 3: Haddon-Cave Report on the Nimrod Accident - 'Bow-Tie' and Swiss-Cheese analogy

As with the Space Shuttle disasters the Nimrod Accident resulted from technical issues and organisational failings. Common issues arose over time (for both Shuttle and Nimrod) as 'latent' failures including:

- Normalisation of risk (Nimrod Project Team/Designers and NASA)
- Incorrect safety assessment and classification of hazards (and their associated accident risk) – (Nimrod and arguably NASA)
- Design changes not formally re-assessed for safety risks (Nimrod air refuelling equipment
- Budgetary and Timeline constraints (Nimrod and NASA)
- Flying aircraft in different context (environment) to which it was designed (Nimrod)

On the day of the accidents 'active' failures played a contributory part and these included:

- Poor management decision to launch (Challenger) – temperatures outside of limits

- Poor management decision to re-enter (Columbia) – could have saved crew by rescue mission to the ISS instead
- Poor awareness of aircraft limitations and 'push-on' military mentality – relating to Nimrod and pressure in the air refuelling system (and normal fuel system) with aging aircraft flying at height in high temperatures being refuelled at high pressure

The accident sequence or chain for the Space Shuttles or Nimrod could have been broken at any point in the latent or active failures detailed above and this is the role of a proactive Safety Management System whereby everyone is aware of safety and anyone can break the 'chain' (discussed further in 2.2.9).

2.1.1.4 Space-Related Accident Trends & Comparisons

It is important to try and understand why accidents have occurred within specific fields and as with the Nimrod accident, a comparison of other similar industries can also be helpful.

A comparison of accidents was provided in Van Pelten's Space Tourism book [10] where he cites the two Space Shuttle Disasters (Challenger 1986 & Columbia 2003) and also 2 Russian Accidents (1967 & 1971). The book is aimed at the general public and therefore provides interesting facts regarding the history of spaceflight and then takes the reader (as a spaceflight participant) on a journey to their spaceflight, covering a theoretical medical and training journey. The following summary table of manned spacecraft Accidents is based on the accidents noted in Van Pelton's book, the NASA library [11] and the Roscosmos website [12]:

Date	Spacecraft	Accident	Flight Phase	Details/Comments
Apr 23 1967	SOYUZ 1	Uncontrolled Crash	Descent and Land	Parachute fails to open resulting in **death of the cosmonaut** (1 on board)
June 06 1971	SOYUZ 11	Structural failure	Re-entry/Descent	Pressure leak in the cabin resulted in the death of **3 cosmonauts**
Jan 28 1986	SPACE SHUTTLE Challenger	Explosion	Launch	Launch temperature too low and O-rings failed resulting in **7 astronaut** deaths
Feb 01 2003	SPACE SHUTTLE Columbia	Structural failure	Re-entry	Damage to wing leading edge from detached foam insulation during launch results in wing disintegrating on re-entry with consequence of deaths of all **7 astronauts**

Table 2: Summary of Manned Spacecraft Accidents

There has already been one accident in the emerging Space Tourism field; this was during a ground test of Scaled Composites' hybrid rocket engine; the test was a nitrous oxide injector test and the System exploded killing three of their engine sub-contractor's scientists. The company provided a statement [13] detailing their plans for continuous improvement including:

- *Conducting increased compatibility testing between N2O and any materials that contact it in the tank and eliminate incompatible materials in the flow path;*
- *Revising cleaning procedures to further minimize the risk of contaminants in the system;*
- *Replacing the composite liner in the N2O tank with a metal tank liner;*
- *Diluting N2O vapour in the tank with Nitrogen or another inert gas to decrease its volatility and/or act as a pressurant;*

- *Designing additional safety systems for the N2O tank to minimize the danger due to tank overpressure; for example, a burst disk feature; and*
- *Increasing the amount of testing during the development program to demonstrate that these design changes, and any improvements to system components, prevent the sequence of events that led to the accident.*

These intended actions appear good means of mitigation against the hazard of explosion including a mix of design modification and safety features and also procedural controls. The question that remains is why was this not done in the first instance i.e. within a formal Safety Management System with integrated design systems safety analysis because surely these mitigation measures would have been identified in a formal hazard identification and analysis process such as a Functional Hazard Analysis?

This accident at Scaled Composites is the only major occurrence that has happened; there has also been a minor incident with White Knight 2 (the carrier aircraft) during a landing run where the left hand landing gear failed. So already during the development stage there has been one fatal accident (with 3 fatalities) and 1 minor reportable incident. When reviewing this against Figure 4 and Figure 5 we can see that there are probably many more incidents that have occurred; the question is 'how are they managing the risks?'

Indeed when examining accident data it is also useful and relevant to examine the 'near misses' (serious incidents) during spaceflights and also to examine those accidents and serious incidents that occur during spaceflight training and during the design and development (in particular, testing as detailed above in the Scaled Composites' accident):

Date	Spacecraft Or Equipment	Accident Or Serious Incident	Flight Phase Or Training Or Testing	Details/Comments
Oct 24 1960	Soviet R-16 missile (included as technology relevant to development of SOYUZ rockets)	Explosion	Launch pad test flight	Second stage motors ignited prematurely killing over **100 people**
Mar 23 1961	Oxygen Chamber	Fire	Low pressure chamber testing	Cosmonaut received burns and **later died**
Apr 14 1964	DELTA Rocket	Explosion	Assembly Phase	Static electricity spark ignited the rocket **killing 3 technicians** and injuring 9 others
Jan 27 1967	APOLLO 1	Fire	Launch Test	Fire during Launch Pad Test resulting in **all 3 astronauts suffocating to death**
Nov 15 1967	X-15	Loss of Control	Training - Descent	Loss of situational awareness resulting in yawing and spin and irrecoverable LOC resulting in the aircraft breaking up at high Mach numbers whilst inverted and not in control – pilot death
May 06 1968	Lunar Landing Research Vehicle (LLRV)	Crash (Loss of control or thrust)	Training – Lunar Landing	Pilot Neil Armstrong ejected safely
Dec 08 1968	Lunar Landing Research Vehicle (LLRV)	Crash (Loss of control or thrust)	Training – Lunar Landing	Pilot ejected safely
1969 January 18	SOYUZ 5	Loss of Control - separation failure	Re-entry	The Soyuz had a harrowing re-entry and landing when the capsule's service module initially refused to separate, causing the spacecraft to begin re-entry faced the wrong way. The service module broke away before the capsule would have been destroyed, and

Date	Spacecraft Or Equipment	Accident Or Serious Incident	Flight Phase Or Training Or Testing	Details/Comments
				so it made a rough but survivable landing far off course in the Ural Mountains
Apr 23 1970	APOLLO 13	Explosion	Orbit	Electrical arc/spark in oxygen system of command module – no deaths as they managed to survive and return to Earth
Jan 29 1971	Lunar Landing Research Vehicle (LLRV)	Crash (Loss of control or thrust)	Training – Lunar Landing	Pilot ejected safely
1975	SOYUZ 18	Loss of Control	Ascent	Non-nominal event resulting in crew experiencing 21g and they used the abort system (emergency escape rockets firing the cabin away from the launcher) – no deaths
Oct 16 1976	SOYUZ 23	Landing capsule sank in water	Landing	The SOYUZ capsule broke through the surface of a frozen lake and was dragged underwater by its parachute. The crew was saved after a very difficult rescue operation.
Mar 19 1981	SPACE SHUTTLE Columbia	Anoxia	Preparation for STS-1	Anoxia due to nitrogen atmosphere in the aft engine compartment: **2 killed** and 3 revived
1983	SOYUZ T-10	Explosion	Launch Pad	Uncontrolled Rocket fire and the crew aborted using the flight safety abort system propelling them away from danger – they were subject to 16g
July 29 1985	SPACE SHUTTLE Challenger (STS 51-F)	Fire	Ascent	Five minutes and 45 seconds into ascent, one of three shuttle main engines aboard *Challenger* shut down prematurely due to a spurious high temperature reading. At about the same time, a second main engine almost shut down from a similar problem, but this was observed and inhibited by a fast acting flight controller. The failure resulted in an Abort to Orbit (ATO) trajectory, whereby the shuttle achieves a lower than planned orbital altitude. Had the second engine failed within about 20 seconds of the first, a Transatlantic Landing (TAL) abort might have been necessary. (No bailout option existed until after mission STS-51-L (Challenger disaster), but even today a bailout—a "contingency abort", would never be considered when an "intact abort" option exists, and after five minutes of normal flight it would always exist unless a serious flight control failure prevailed
July 23 1999	SPACE SHUTTLE Columbia (STS-93)	Main engine electrical short and hydrogen leak	Launch-Ascent	Five seconds after lift-off, an electrical short knocked out controllers for two shuttle main engines. The engines automatically switched to their backup controllers. Had a further short shut down two engines, *Columbia* would have ditched in the ocean, although the crew could have possibly bailed out. Concurrently a pin came loose inside one engine and ruptured a cooling line, allowing a hydrogen fuel leak. This caused premature fuel exhaustion, but the vehicle safely achieved a slightly lower orbit. Had the

Date	Spacecraft Or Equipment	Accident Or Serious Incident	Flight Phase Or Training Or Testing	Details/Comments
				failure propagated further, a risky transatlantic or RTLS abort would have been required.
Aug 22 2003	VLS-1-301 Rocket	Explosion	Launch Pad	One of four first stage motors ignited accidentally – **killing 21** people
July 26 2007	SPACESHIP 2 Hybrid Rocket	Explosion	Engine Test bed	the test was a nitrous oxide injector test killing **3 people**
April 19 2008	SOYUZ TMA-11	Loss of Control	Re-entry	Suffered a re-entry mishap similar to that suffered by Soyuz 5 in 1969. The service module failed to completely separate from the re-entry vehicle and caused it to face the wrong way during the early portion of aero-braking. As with Soyuz 5, the service module eventually separated and the re-entry vehicle completed a rough but survivable landing.

Table 3: Summary of Manned Spaceflight-Related Accident and Serious Incidents (non-flight)

There have been circa 281 missions to date [14] and therefore the average fatal accident rate is 1 in 70 per mission.

In terms of people, the risk of death for astronauts is about 4 per cent (18 out of 430 astronauts that have flown on operational flights). From the first launch of Yuri Gagarin to the present day there have been circa 133 fatalities; it is not known how many people have been involved and how many 'activities' were undertaken and so it is difficult to be accurate with the statistics.

A comparison with aviation and risky activities such as parachuting averages a risk of death of 1 in 100,000 jumps for parachutists and 1 in 2 Million flights for aviation passengers. So NASA's safety performance of 1 in 70 is concerning and is clearly a target to vastly improve on for the nascent suborbital domain.

The statistical trends and comparisons can certainly be useful in determining safety criteria (see 2.3.1.1) and this should arguably be derived by the regulators for use in policies and guidelines.

Table 3 details the reported accidents and serious incidents within the space domain and when we consider the 'iceberg model' and apply the Heinrich ratio in Figure 4 a picture starts to emerge of the underlying safety risks that may or may not be being managed effectively.

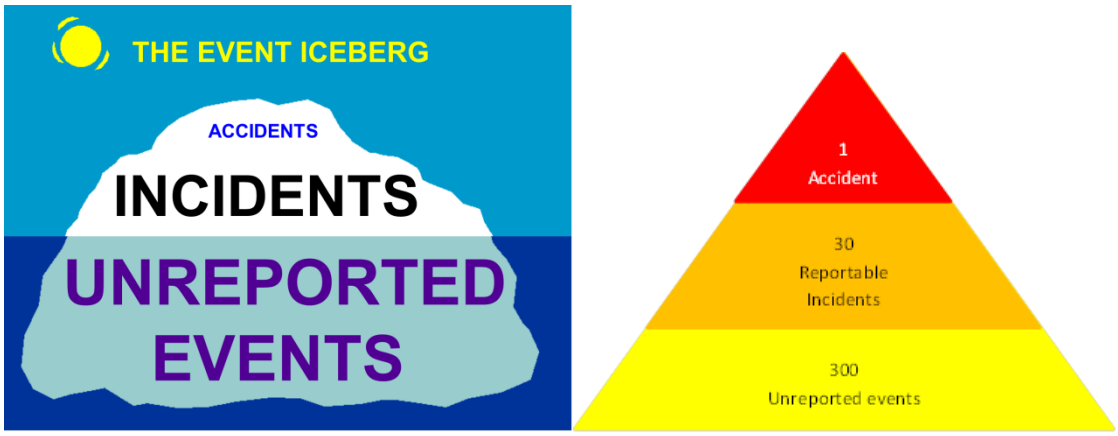


Figure 4: Standard Iceberg Model - Heinrich Ratio

The updated Heinrich ratio examines the relationship between accidents and incidents and adds an additional layer. For the purpose of space or aviation this extra layer is more appropriate as it considers fatal accidents, accidents and reportable incidents (as well as the unreported incidents). Figure 5 represents the added layer and we can then get a better perspective on the safety risks involved. In terms of a safety culture one cannot merely gauge this on the number of accidents that have occurred i.e. an airline may have not had any fatal accidents but may be experiencing 100 Air Safety Reports per month and ten per cent of these may be significant (safety significant events). On top of that there may be hundreds of near misses in regards to ground incidents as well as incidents in the air. Thus it can be seen that aviation and space flights carry a high safety risk and this needs to be a) recognised and b) managed.

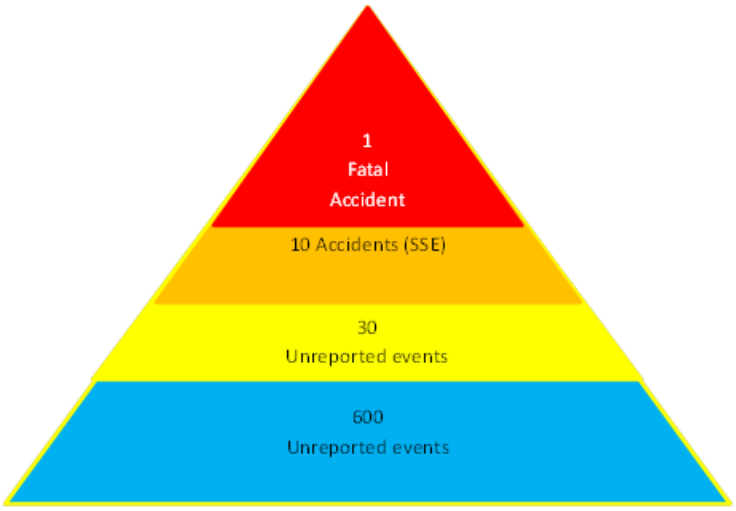


Figure 5: Updated Heinrich Ratio showing accidents (safety significant events)

The statistics are important to gain an understanding regarding the industry risks yet need to be viewed in 'like terms' for the emerging Personal Spaceflight field. The Shuttle for instance is a vertical take-off/horizontal land vehicle, whereas the APPOLLO and SOYUZ are Vertical take-off/Vertical Land vehicles. Within aviation, the aeroplanes are horizontal take-off/horizontal (powered) landing. There will be different combinations for suborbital operations in the near future and one of the leaders (Virgin Galactic) has a totally different profile of horizontal (airborne) take-off/vertical descent and horizontal (non-powered) approach and landing. In his extremely biased and journalistic book (published by Virgin Books Limited), Kenny Kemp [15] talks to key players from Virgin Galactic (VG) who categorically believe that their innovative System is 'safe':

- Will Whitehorn (VG President) – *'Safety is and will continue to be Virgin Galactic's North Star'*
- Burt Rutan (Scaled Composites) – *'We believe a proper goal for safety is a record that was achieved during the first five years of commercial scheduled airline service, which while exposing the passengers to high risks by today's standards, was more than a hundred times safe as government manned space flight'*
- George Whitesides (then VG Chief Technical Officer, now Chief Executive Officer) – *'So now you have a hybrid [rocket motor] which is extremely safe at low cost and with an efficiency that is in between solids and liquids. So it is ideal technology for us'.*

The Virgin Galactic air-launch system may have many inherent safety features in its design and only time will tell of its success during test flights and during the early phases of commercial operations.

However the development program has come at a high cost; as detailed in Table 3 above, there was an accident during Scaled Composites' testing of their hybrid rocket system where 3 scientists were killed and others severely injured in an explosion.

The XCOR 'Lynx' RLV is a horizontal take-off/horizontal land (powered ability) craft and the airframe is designed and built more conventionally, therefore one could argue that the XCOR vehicle is the safest proposal thus far; except that its profile dictates use of a rocket engine for take-off and therefore is susceptible to high risks on the ground. The rocket design is unique in that it has the ability to terminate the thrust phase (to conduct an abort scenario) but then also has the capability to re-ignite[8] (to either continue with the flight or to assist in controlling the vehicle or indeed to fly to another nearby landing location). This therefore could be seen as an advantage in that the rocket engine is initiated on the ground and their procedures could dictate that the brakes are not released until satisfactory pressures and temperatures are verified.

The risks faced by the newcomers to the space industry will be similar in nature to those faced by NASA and it will be interesting to see if the 'lessons identified' from the Space Shuttle disasters will indeed influence the management in the suborbital domain.

The role of Management will play a large part in the success or failure of a suborbital mission. Management can directly influence many aspects including:

- Launch 'Go/No-Go' decisions – 'Active' failure as in the Challenger disaster
- Sign-off for System's Exceptions and Limitations – 'Active' failure on the day, but also 'Latent' failure in the case of NASA because this was the 'norm' over a long period of time as cited by Diane Vaughan (*….in fact the listing and description of the ''acceptable risks'' on the Space Shuttle prior to the first launch in April 1981 filled six volumes)*
- Operating Profile decisions
- Design Acceptance decisions
- Influence on design

2.1.2 Spaceflight Conferences

Spaceflight-related conferences have recently provided organisations and individuals an opportunity to discuss Personal Spaceflight as well as the Governmentally-led safety topics concerning the International Space Station (ISS) activities and the Space Shuttle replacement program.

The author has attended and presented papers at the International Astronautical Conference (IAC) and also the International Association for the Advancement of Space Safety (IAASS). Although the majority of the proceedings' concern governmental programs there is growing interest in the emerging commercial spaceflight field; indeed the IAASS expressed 'concern' over the 'newcomers' to Space.

The IAASS Independent Space Safety Board (ISSB) has produced a 'Space Safety Standard – Commercial Manned Spacecraft' [16] to provide guidance to the new community. Its purpose is to '*establish safety requirements applicable to the IAASS Certification of Commercial Human Rated Systems (CHS)*'; this covers both orbital and suborbital spaceflight. Interestingly, the scope covers flight personnel (crew and spaceflight participants), ground personnel, the vehicle and any other interfacing system from the CHS-related hazards. It furthermore excludes the Expendable Launchers and all issues relating to public safety. This is in discord with the governmental-driven programmes

[8] http://www.xcor.com

and safety analysis and also in the FAA-AST commercial spaceflight guidelines; both of these approaches focus heavily on protecting the public and use the 'Expected Casualty [Ec]' methodology (see Section 2.3 below). The ISSB Manual also appears to be in discord with the 'Safety Risk' criteria stating that:

- *for orbital flights the probability of a catastrophic event for the flight personnel during the entire mission shall not exceed 1x10-3*
- *for suborbital flights the probability of a catastrophic event for the flight personnel during the entire mission shall not exceed 1x10-4*

There is no explanation as to how these values were derived and therefore one could interpret these values in different ways i.e. it could mean the Total Safety Risk (sum of all accidents over the whole duration of the mission) or it could mean the value for catastrophic failure conditions.

The rest of the ISSB Manual identifies Technical Requirements (Chapter 2), Vehicle Safety Design Requirement (Chapter 3) and Certification Requirements (Chapter 4).

Another relevant conference is the International Academy of Aeronautics (IAA) and their first conference was in 2008 at Arcachon, France; the main theme was that the industry needed proper regulation and main operators presented their hypothetical spacecraft and trajectories. The 2nd IAA conference on 'private commercial spaceflight' provided updates to the original themes and the sessions were split into legal/regulatory and designer/operator business models. A common issue was identified in both sessions in that the FAA-AST 'launch licensing' methodology was in contradiction to the proposed European Aviation Safety Agency (EASA) certification methodology (for winged aircraft – see 2.3.8). The designers were split in that the US-based companies such as XCOR and Rocketplane wanted to fly in Europe but remaining under the FAA-AST remit whereas European-based companies such as EADS-Astrium and Reaction Engines wanted to be certified by EASA. The rationale from the US-based companies was that the EASA certification approach is more protracted, more costly (by an order of magnitude) and would be difficult to achieve the safety objectives for failure conditions i.e. to provide evidence of meeting in the order of 1×10^{-7} per flying hour for example. Reaction Engines are actually designing an orbital spacecraft (Skylon) but they want EASA certification. They at least have attempted to derive probabilities for catastrophic failure conditions by using an 'abort' rate and linking this to a platform loss rate. The approach appears sound and will be discussed in 2.2.6. One problem with Reaction Engines wanting to be certified by EASA is that the agency are only proposing to certify winged vehicles (which Skylon is) up to the edge of space i.e. within the 'air domain'; EASA state they are not competent to certify a vehicle in the 'space domain'. It shall be also noted that currently, the FAA-AST responsibility is limited to the launch and re-entry phases of the flight, and not to the phase in-between, i.e. the orbital flight phase. Herein lays the problem for Reaction Engines in that the majority of their flight will be in the space domain; of course they have to fly through the air domain for the climb and when they enter the re-entry phase. The author contends that a dual-approach will have to be taken in that EASA could certify the air domain aspects and another 'suitable' authority will have to approve and manage the space domain aspects; this later space domain issue has not been addressed sufficiently by the Industry at this time. This is further discussed in the 'space law' versus 'air law' debate in 2.3.9.

2.1.2.1 Papers

The author has submitted spaceflight-related papers to conferences during the period of the Thesis and these have been focussed on the perceived gaps in the emerging space tourism industry. The following papers were authored during the period and are included in Appendices 8 through 12:

- Oct 2006, *SMS for the Private Space Industry*; submitted to the IAC in Valencia
- May 2007, Certification of microgravity flights in the UK; presented to the UK CAA as an internal paper for QinetiQ
- Oct 2008, Centrifuge as key mitigation in the private spaceflight industry; submitted to the 3rd IAASS in Rome
- May 2010, Safety Criteria for the Personal Spaceflight Industry; submitted to the 4th IAASS in Huntsville
- Oct 2011, Safety Model for the Commercial Spaceflight Industry; being submitted to the 5th IAASS in Paris

The relevance of the papers is that a thorough review of the industry and academic literature was undertaken for each paper in addition to and complementary to this Thesis.

2.1.3 Spaceflight Conclusion of Academic Review

It is clear that academia and industry bodies are both concerned and excited at the prospect of the emerging Space Tourism industry. There is trepidation in that accidents may occur as per those that have occurred either on launch or during re-entry. There are fundamental safety culture issues that have been raised in terms of Normalisation of Risk. These Lesson Learnt (or rather Lessons Identified) must be captured, digested and instilled in the new industry. This aspect will certainly be one of the objectives of a new Technical Committee of the International Association for the Advancement of Space Safety (IAASS) – which the author has instigated and will Chair (see Chapter 3).

The various papers presented at space safety conferences reflect a changing attitude towards safety in that no more is safety an afterthought to NASA-based projects and this is being instilled amongst their European and other Nation brethren (as opposed to engineer the solution with a bit of Human Machine Integration and finally can we get safety 'sign-off').

The popular books that are on the market tend to be fanciful and have been released too early (possibly in anticipation of a 2007 launch from Virgin Galactic); here we are approaching five years later and more to the wise on what is required in terms of passenger training (2.3.6) and medical requirements (2.3.4).

There are plenty of theoretical ideas on safety and design but it boils down to what the safety requirements are and what the safety targets are; these aspects are still being considered by designers and regulators alike and is the main topic of this Thesis.

2.2. **REVIEW OF SAFETY MANAGEMENT 'TOOLS'**

2.2.1 Safety Management Systems

It is first important to clarify what is meant by a 'System'. According to the Oxford Advanced Learners Dictionary [19] a system means:

> *"an organised set of ideas or theories or a particular way of doing; a group of things, pieces of equipment, etc., that are connected or work together, or; the rules or people that control a country or an organisation"*

From the above definition of 'system' we can discern that there is a common thread – organised approach, connected and controlling. So when we apply this to 'Safety Management System' we are concerned with the safety approach an organization takes to control an activity or function.

Safety Management is a proactive safety-based activity with the purpose of accident and incident prevention by means of prospective analysis. Flight Safety on the other hand could be considered as reactive events from or during an incident; a pilot of an RLV can be considered managing the Flight Safety during an Incident (and actions prior to or preventing the incident) and Flight Safety Officers on the ground would then record the Incident for further investigation and trend analysis by means of retrospective analysis. Arguably both types of activity should be employed in a complimentary organisational 'system' within the Personal Spaceflight Industry in order to capture the 'Lessons Learnt'; not only from the Aviation Industry, but other Industries such as the Rail and Petro-Chemical Industries. All of these Industries have complex and critical aspects to their modus of operand and all have suffered Catastrophic Accidents where safety issues were cited as major contributory factors. Indeed in 1988 the UK suffered 2 such accidents; the Piper Alpha Oil Rig disaster and the Clapham Junction Railway accident. Following these events and as a result of the findings from the subsequent investigations from the Lord Cullen report [20] and a general need to improve railway safety regulations [23], safety cases were introduced as requirements for these industries as part of an effective SMS.

More specifically related the Challenger disaster may have been averted had a more robust SMS been in place; Diane Vaughan [7] cited a 'poor safety culture' referring to NASA's safety policies (allowing 'six volumes' of 'acceptable risks' on the Space Shuttle) and NASA's processes (the Management decision to launch against engineering advice).

From the mid-90's onwards the proactive SMS models were introduced and the International Civil Aviation Organisation's document [24] (ICAO 9859 – Safety Management Manual) presents a mix of the reactive and proactive methods. The ICAO is the overarching SMS guidance document and the following definitions of SMS are from varying governing bodies and prominent safety standard documents.

The UK Civil Aviation Authority (CAA) updated their SMS Publication to an SMS 'Guidance to Organisations' [25] document that aligns with ICAO Manual and the CAA defines an SMS as:

> *"An SMS is an organised approach to managing safety, including the necessary organisational structures, accountabilities, policies and procedures. The complexity of the SMS should match the organisation's requirements for managing safety. At the core of the SMS is a formal Risk Management process that identifies hazard and assesses and mitigates risk."*

The CAA document is aimed at Air Operator Certificate (AOC) holders and Aerospace Maintenance Organisations.

The FAA definition from the SMS Advisory Circular [26]:

> *"The formal, top-down business-like approach to managing safety risk. It includes systematic procedures, practices, and policies for the management of safety (including safety risk management, safety policy, safety assurance, and safety promotion)."*

The Euro Control 'SKYbrary' [27] definition:

> *"Safety management is an organizational function, which ensures that all safety risks have been identified, assessed and satisfactorily mitigated."*

Defence-Standard 00-56 [28] definition:

> *"The organizational structure, processes, procedures and methodologies that enable the direction and control of activities necessary to meet safety requirements and safety policy objectives"*

The relevance to this Thesis is to ascertain a 'best practice' SMS definition in order to clarify what an SMS is. Taking the relevant phrases from each definition helps narrow the process:

- *Organised approach*
- *Formal top-down business-like approach*
- *Organizational function*
- *Safety organization structures, safety policies and systematic safety procedures*
- *Formal Safety Risk Management*
- *Meeting Safety Requirements*

From the above list we derive the Thesis definition:

A Safety Management System is a safety organizational function concerned with implementing and managing safety policies and procedures necessary to undertake formal safety risk management

2.2.2 Safety Management Plan

Now that SMS definitions have been presented, the underpinning organizational document that details the SMS is the Safety Management Plan (SMP).

The documents reviewed to assess the SMS definitions have been reviewed to assess the suggested SMP contents. The ICAO 9859 Manual [24] suggests that an SMS Manual (SMSM) and an SMS Implementation Plan is required; the former being an instrument for communicating the SMS approach to the whole organization and the Implementation Plan (SMSIP) defines the organization's approach to managing safety. The SMSM suggests the following contents:

- *scope of the safety management system;*
- *safety policy and objectives;*
- *safety accountabilities;*
- *key safety personnel;*
- *documentation control procedures;*
- *coordination of emergency response planning;*
- *hazard identification and risk management schemes;*

- *safety assurance;*
- *safety performance monitoring;*
- *safety auditing;*
- *management of change;*
- *safety promotion; and*
- *Contracted activities.*

The SMSIP suggests the following contents:

- *safety policy and objectives;*
- *system description;*
- *gap analysis;*
- *SMS components;*
- *safety roles and responsibilities;*
- *hazard reporting policy;*
- *means of employee involvement;*
- *safety performance measurement;*
- *safety communication;*
- *safety training; and*
- *management review of safety performance*

The Def-Stan 00-56 [28] document focuses on providing guidance on establishing a means of complying with the Requirements for the management of Safety; hence although many of the ICAO contents are included, Def-Stan 00-56 additionally suggests:

- *Initial definition of all key Safety Requirements*
- *Tolerability Criteria*
- *Safety Programme Plan*
- *Compliance Matrix*

Both the EASA [27] and FAA [29] documents defer to the higher ICAO (1) SMSM in that they follow the four-tiered SMS component/framework approach:

- *Safety policy and objectives*
- *Safety Risk Management*
  - *Hazard Identification*
  - *Risk Assessment and Mitigation*
- *Safety Assurance*
  - *Safety performance monitoring and measurement*
  - *The management of change*
  - *Continuous Improvement of the SMS*
- *Safety Promotion*

The relevance to this Thesis is to ascertain a ‘best-practice’ SMP suggested content list. From the above review it is clear that the ICAO, EASA and FAA methodology omit a vital element that has been covered by the Def-Stan 00-56 approach: Safety Requirements, including Tolerability Criteria.

The SMP should describe the following as a minimum[9]:

- Safety Policy & Objectives
- Safety Organisation, Roles & Accountabilities/Responsibilities

[9] The SMP List is compiled by the author as ‘best practice’ combining relevant aspects from the following documents: References 24, 25, 26, 27 & 28.

- A description of the Safety Management System to be operated
- Note: in this instance, an RLV Operator's SMS will include a description of the SMS approach by the organization towards formal safety risk management
- A description of the RLV Equipment
- Scope of the SMS including details of interface SMSs or Safety Cases
- Safety Programme Plan
- Initial definition of all key Safety Requirements
- Tolerability Criteria
- Hazard and Risk Management Approach
- Occurrence Management
- Emergency Response Plan
- Safety Audit Plan
- Safety Promotion
- Change Management Plan (including Configuration Control)
- Compliance Matrix
- Contractor Requirements

2.2.3 The Safety Case

The Safety Case has been adopted within the UK as a result of catastrophic accidents mentioned in 2.1.1.3. Within Def-Stan 00-56 [28] a safety case is defined as:

> *"A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment"*

Safety Cases may be produced at the System, Super-System or Sub-System level. Where lower-level Safety Cases require integration to the prime System or Super-System Safety Case then the prime organisation should be responsible for ensuring that an Integration Safety Case or Safety Case Report may be required to ensure there are no weaknesses to the argument; invariably through experience, the author has found many weaknesses at the boundary between Safety Cases.

There are several ways to construct a Safety Case in terms of structure and expression and this depends on the scale and depth of the Safety Case.

A safety argument may be made textually if a simple system is being argued as 'safe' i.e. the argument is familiar and uses standard evidence from the domain such as a Certificate of Design (see Figure 6 below). However at the other end of the scale a 'System' may be in the Space Tourism domain whereby the technology and environment are unfamiliar and there are no known standards; in this instance a Safety Case is recommended and possibly using both textual and Claims-Arguments-Evidence (CAE) diagrams or Goal Structuring Notation (GSN) to demonstrate that the 'System' is safe.

		Solution	
		Familiar	**Unfamiliar**
Problem	**Familiar**	Minimal argument and standard evidence from the domain i.e. certificates of design	Focused argument on reasons for novel solution, plus the appropriate evidence
	Unfamiliar	Minimal argument and standard evidence from another domain i.e. use of FAA/NASA standards	Extensive argument and evidence, with substantial independent scrutiny and application of novel standards and technology i.e. Space Tourism Operations

Figure 6: Complexity of 'System' and Requirements for structured argument and evidence

2.2.3.1 Safety Case Boundaries

The scope of the safety case is an important starting point and must be explicit in detailing the boundaries. Once the scope has been defined then further assumptions can be made as to the use of the System; these will be numerous in the beginning of a project but as the development progresses these should be replaced by evidence.

- Design Organisation Safety Case (platform level); this is the 'As Designed' safety case covering the design, certification, manufacture and test of the platform. Feeding into the Platform Safety Case (As Designed) are lower-level sub-system safety cases i.e. for the Avionics system, Engine System, Hydraulic System and so on:
  - Sub-System Safety Case (system 1)
  - Sub-System Safety Case (system 'n')
- Integration Safety Case; this is an essential aspect to consider because in the case of engines (as a sub-system) they will have their own DO safety case which needs to be analysed for its integration on a particular aircraft and operated and supported in certain environments. Aspects to consider include;
  - Maintenance activities
  - Operating environment such as Air Traffic and Spaceport safety
  - Support Equipment i.e. Specialist Ground Support Equipment such as propellant loaders
- Operator Safety Case; this is the 'As Flown' safety case incorporating operational aspects such as;
  - operating environment
  - operator procedures
  - operator limitations
  - operator training
  - operator safety risk management

Figure 7 below depicts the integration of safety cases at different levels; in this instance it is for a Suborbital Aircraft with Carrier Aircraft. The sub-systems below the SoA level should have their own safety cases and one of the most important facets of the 'Total Safety Case' below is the integration argument. The Rocket Propulsion System (RPS) may be procured as a bespoke system and therefore may have reliability data and service history to form the backbone of its safety case but is the RPS safe within the context of the SoA. Likewise the Carrier Aircraft will have its own safety case and certification but a modification will be required to integrate the SoA with the Carrier (either top-

loaded or bottom-loaded) and it is this system that will require an additional integration safety case argument.

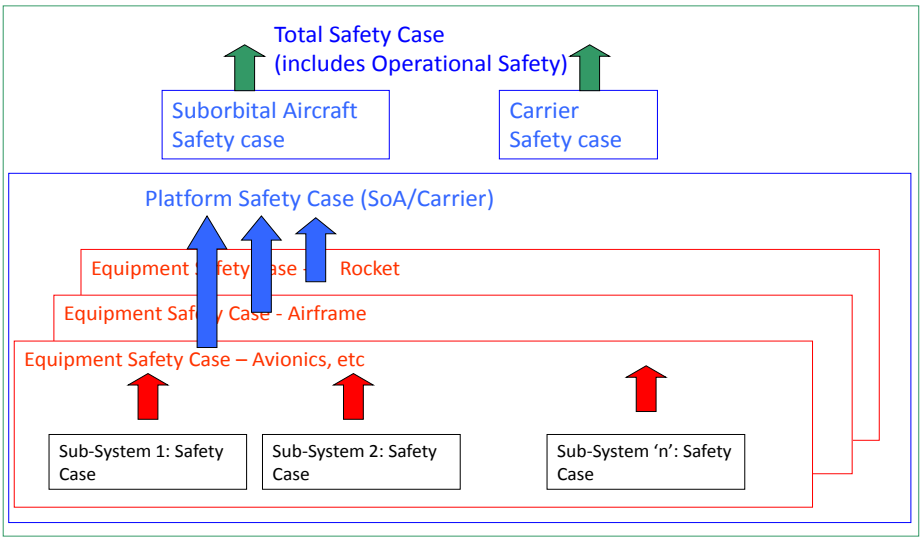


Figure 7: Integrated Safety Case Approach

2.2.3.2 The Safety Case Report

The Safety Case Report (SCR) is a document that presents a safety argument of the Safety Case as a 'snapshot' in time; therefore it is a document that should be updated throughout the development of the spacecraft, throughout its life and also at disposal of the spacecraft (or de-commissioning of spacecraft or sub-systems as part of the fleet). UK Def-Stan 00-56, Issue 4 suggest that a SCR should report on the following project aspects:

- *Executive Summary*
- *System Description*
- *Progress against the (Safety) Programme*
- *Hazard Analysis (including mitigation)*
- *Emergency/Contingency Arrangements*
- *Operational Information*
- *Audit Reports*
- *Conclusions/Recommendations*

The SCR is a vital document in tracking the progress and also in tracking discrepancies and observations as the project advances. It is also a formal and auditable record of safety activities undertaken since the last SCR. It provides the Accountable manager with a summary of the progress and importantly whether the safety risks are acceptable and being managed.

In terms of the design lifecycle there are important milestones (such as Preliminary and Critical Design Review, etc.) and so the safety case can be summarised at those milestones in the form of the SCR. Figure 32 details the design 'Vee' lifecycle and the SCR submissions can be seen as the program develops.

2.2.4 Hazard Management

The Hazard Management System (HMS) is vital to the success of the safety effort and the Hazard Log is the core of the HMS as it is the final suppository of safety information and should provide a means of tracking hazards and assist in providing a means of assessing the overall risk of the spacecraft so as

to measure whether the safety target has been met. It is important to define the basics such as defining what a hazard is and to understand its sequential position within the accident sequence:

Hazard definitions:

- FAA AC [18]; *Equipment, system, operation or condition with an existing or potential condition that may result in loss or harm*
- UK Def-Stan 00-56 [28]; *A physical situation or state of a system, often following from some initiating event, that may lead to an accident*
- ICAO SMS Manual [24]; *A condition or an object with the potential to cause injuries to personnel, damage to equipment or structures, loss of material or reduction of ability to perform a prescribed function*

Cause definitions:

- FAA AC [18]; the Advisory Circular has 'FAULT' as an initiating event and define it as '*an anomalous change in state of an item that may warrant some type of corrective action to decrease risk.*'
- UK Def-Stan 00-56 [28]; *the origin, sequence or combination of circumstances leading to an event*
- ICAO SMS Manual [24]; does not contain a definition of a Cause or 'Fault' but note that each hazard will have a unique set of '*CAUSAL FACTORS'*.

Accident definitions:

- FAA-AST AC [18] does not define accident. They have 'MISHAP' defined as; '*a launch or re-entry accident, launch or re-entry incident. Launch site accident, failure to complete a launch or re-entry as planned, or an unplanned event or series of events resulting in a fatality, serious injury, or greater than $25,000 worth of damage to the payload, launch or re-entry vehicle, launch or re-entry support facility, or governmental property located on the launch or re-entry site*.'

The FAA-AST AC [18] paragraph 5b says to classify the RISK of the hazard by its severity and likelihood – hence their concept is to recognise that the hazard has a probability but it also contains a severity element i.e. to the event's outcome or consequence. The issue here is that there is no explicit link to a particular accident and therefore how do you manage the 'category B' defences (recovery barriers in the Haddon-Cave model in Figure 3)?

Failure Condition definition:

However for aircraft certification purposes we have failure conditions and these are linked to a severity classification (and not a specific accident). The failure condition is defined [87] as:

> *A condition having an effect on either the airplane or its occupants, or both, either direct or consequential which is caused or contributed to by one or more failures or errors considering flight phase and relevant adverse operational or environmental conditions or external events*

In this instance failure conditions have been derived from Functional Hazard Analysis (see 2.2.4 below) and therefore have known consequences; thus designers know that a '*misleading airspeed display'* failure condition could lead to a catastrophic event and therefore must met the relevant safety objective ($1x10^{-9}$ per flying hour).

It is notable that there appears to be little difference between a ‘hazard’ and a ‘failure condition’ from the above descriptions and this could lead to problems. This is discussed further below in ‘accident sequence’ section 2.2.5.

2.2.4.1 Hazard Identification & Analysis

The Hazard Identification & Analysis (HIA) process should start at the beginning of a program and continue throughout the life of the program up to ‘Disposal’. Figure 8 below shows different phases of a program and typical safety activities undertaken at each stage.

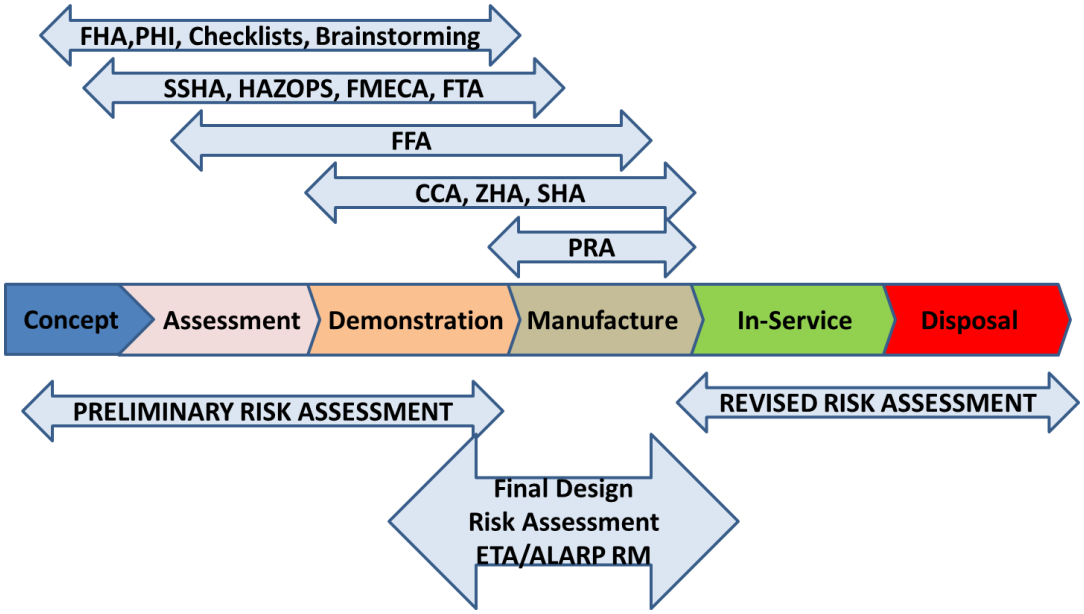


Figure 8: Design Cycle detailing typical stages and associated safety activities

The design cycle shown above compliments the standard ‘V-Model’ design phases for Validation and Verification as detailed in section 2.2.16.

Design Organisations (DO) follow best practices and must meet certification requirements for their aircraft i.e. Joint Airworthiness Regulations (JAR) 25.1309 and accompanying guidelines Advisory Circular (AC) 25.1309-1A for large aeroplanes. DOs also follow guidelines to ensure a consistent and recognised approach has been taken when presenting their analysis to the regulators. Typical guidelines include Aerospace Recommended Practice (ARP) 4761[75] and ARP 4754 [39]. The standard safety analysis techniques include:

Functional Hazard Analysis (FHA)

> *A Functional Hazard Assessment (FHA) is conducted at the beginning of the aircraft/system development cycle. It should identify and classify the failure condition(s) associated with the aircraft functions and combinations of aircraft functions. These failure condition classifications establish the safety objectives.*

The FHA is vital step in the safety process and in particular to a new project such as a suborbital Aircraft (SoA) for spaceflight it is fundamental in ensuring that failure conditions are identified and safety objectives set. This aspect is covered in more detail in 3.2 as part of the EASA Suborbital Aircraft Policy task; this provides an FHA based on Part 23.1309 and adapted for spacecraft (Suborbital Aircraft).

Preliminary System Safety Assessment (PSSA)

> *The PSSA is a systematic examination of the proposed system architecture(s) to determine how failures can cause the functional hazards identified by the FHA. The objective of the PSSA is to establish the safety requirements of the system and to determine that the proposed architecture can reasonably be expected to meet the safety objectives identified by the FHA.*

The PSSA (for functional failures) can be in the form of Fault Tree Analysis (FTA) which can be based on the functions derived from the FHA. The initial FTA can be at the aircraft level and this can be useful in determining budgets (derived safety requirements) on lower-level systems. Then these lower-level systems can have their own FTAs in order to demonstrate that they have met their failure condition's safety objective.

Fault Tree Analysis (FTA)

> *The FTA should be updated throughout the program as more information such as Failure Modes and Effects Analysis (FMEA) becomes available.*

System Safety Assessment (SSA)

The SSA is the same as a System Hazard Analysis (SHA) and the prime purpose of the SSA (SHA) is to determine whether the safety requirements and targets have been met:

> *The System Safety Assessment (SSA) is a systematic, comprehensive evaluation of the implemented system to show that safety objectives from the FHA and derived safety requirements from the PSSA are met.*

An SSA can be undertaken at the aircraft level and also at the system level (Sub-System Safety Assessment).

> *The difference between a PSSA and an SSA is that a PSSA is a method to evaluate proposed architectures and derive system/item safety requirements; whereas the SSA is a verification that the implemented design meets both the qualitative and quantitative safety requirements as defined in the FHA and PSSA.*

Zonal Safety Assessment (ZSA)

A ZSA is a technique that is performed to identify common causes of failure. In essence it is: *"an analysis of the component-external failure modes and their effects on the relevant system itself and adjacent systems."*

The ZSA is an important technique that should be conducted early in the program in the first instance (by use of installation drawings, photographs, etc.) and then undertaken 'on-aircraft' to verify the initial findings and to identify issues as a result of the physical inspection; from the author's experience, actual installations often differ slightly to that of the drawings and chaffing or interference hazards can be more prevalent and easily identified when the aircraft is built. Should 'Rigs' or Mock-ups be available during the development then these can also be used for the ZSA and other safety analysis techniques.

2.2.4.2 Other Hazard Identification and Analyses methods

Other methods of Hazard Identification and Analysis include software and complex hardware aspects and also analysing inherent hazards. Firstly in terms of inherent analysis the Occupational Health Hazard Analysis (OHHA) and the Operating & Support Hazard Analysis (O&SHA) are recognised techniques. These are defined Defence Standard 00-56 [28] as:

Occupational Health Hazard Analysis OHHA

OHHA is carried out to identify health hazards and to recommend measures to be included in the system, such as the provision of ventilation, barriers, protective clothing etc., to reduce the associated risk to a tolerable level.

Additionally the UK MoD recognised the activity and produced guidelines in their Acquisition Operating Framework database [40].

Additionally the UK MoD recognised the activity and produced guidelines in their Acquisition Operating Framework database [40]. Additionally Def-Stan 00-56 Issue 2 [32] provided guidelines on what the analysis should consider such as:

- *The presence or production of toxic, inflammable or explosive materials, e.g. carcinogens or suspected carcinogens, systemic poisons, asphyxiants or respiratory irritants*
- *The generation of noise, vibration, physical shock, electric shock, heat or cold stress, ionizing or non-ionizing radiation*
- *Exposure to the health hazards from other systems*
- *The requirements of the Montreal Protocol, and current UK legislation*

The output of an OHHA activity generally provides causes to known hazards such as ‘exposure to lethal voltages’ or ‘exposure to hazardous materials (absorption)’ but the analysis can also identify new hazards.

An OHHA is normally conducted by means of a checklist/audit approach with the results recorded in either a standalone document or within the SHA.

OSHA

Operating and Support Hazard Analysis is carried out to evaluate hazardous tasks that may be undertaken by operation and support staff. In addition, it should identify the nature and duration of actions that occur under hazardous conditions during various stages of in-service usage such as testing, installation, modification, maintenance, support, transportation, servicing, storage, operation and training.

As with the OHHA the output of an OSHA activity generally provides causes to known hazards but can also identify new hazards. It is important to get the procedures (operating and maintenance) as soon as possible during the development phase so that a ‘desk-top’ analysis can be carried out. Then if Rigs or Mock-ups are available this can be more effectively conducted using the procedures on the actual equipment. The activity must be carried out on the final build stage as procedural steps may not be able to be performed as detailed and it is at this stage that the first amendments can be made so that hazards are not introduced (or human factors [short-cuts] introduced).

Additionally the FAA recognises the activity and has developed a procedure for undertaking an OSHA [41]. The procedure states '*the O&SHA identifies and evaluates hazards resulting from the implementation of operations or tasks performed by persons*.'

The UK Def-Stan 00-56 Issue 2 [32] also provides guidelines for conducting an OSHA and suggests the activity should cover:

> The state of the system including;
>
> - *The interfaces with the system*
> - *The specified range of environmental conditions*
> - *Other associated equipment*
> - *The effect of concurrent tasks and the order and complexity of tasks*
> - ***Ergonomic** issues*
> - *Training issues*
> - *The potential for **human error***
> - *Commitment to safety by line management*
> - *Other **common cause failures**; e.g. human induced error and maintenance procedures.*

Of note the ergonomics, the potential for human error and common cause failures were prevalent within the author's own experience of conducting OSHAs.

Software Safety

Software safety is a specialist subject and within a development program is often worthy of a separate Software Safety Working Group (SSWG) whom report to and sit on the Safety Working Group. Software in itself cannot do anything without a system and so software in itself is not hazardous. It is the requirement to use software within Complex Programmable Equipment (CPE).

Software Development

Software development within an aircraft/spacecraft program is one of the most challenging and difficult aspects to manage and hence a lot of effort must be expended at the beginning to fully understand the requirements otherwise the results could be both costly and catastrophic. The following presents a high level review of software safety aspects.

The standards for software certification and safety are contained in DO-178B [42] and additionally of relevance in the NASA Software Safety Guidebook [43].

The software safety effort within a program starts with a safety program:

- Software Program Plan: a software program plan is the most important document to get right at the beginning of a program that involves software. The plan
- Software Requirements
  - System Requirements – these are platform system requirements at the beginning of the program. From these Safety Requirements and Software Requirements are derived
    - Software Requirements – as with system requirements software requirements are developed from the function of the hardware and its associated function of the embedded software. The software may be performing a command function or indeed it could provide a control function; these need to be specified and then depending on the function and possible outcomes (in terms of hazards) the

requirements can then be refined as to whether the software is a safety critical item or not

- Safety Integrity Levels (SIL) 'v' Design Assurance Levels' (DAL) – these are different levels of assurance required of the software function. The SILs/DALs are produced in different standards as detailed below. Figure 9 details a comparison of the different standards:

SIL	DS 00-55		IEC 61508			DO-178B		DAL
	Justify	Mand-atory	Not Rec	Rec	Highly Rec	Objec-tive	Obj + Indep	
4	0	292	2	1	52	66	25	A
3	17	275	2	14	39	65	14	B
2	115	177	2	30	27	57	2	C
1	120	172	0	29	16	28	2	D
0	-	-	-	-	-	0	0	E

Figure 9: Safety Integrity Levels – Comparison of standards

  - Software Safety Standards – the following standards apply to software
    - DO-178B [42]
    - IEC 61508 [45]
    - Def-Stan 00-56, Issue 2 [32] [now withdrawn]
  - Safety Critical Requirements – *Safety Critical Software includes hazardous software (which can directly contribute to a hazard)* [NASA guidebook - 43]; these also include software in as a control function
  - Non-safety critical requirements
- Fault Tolerance requirements
  - Detailed in the main safety validation matrix – whereby software fault tolerance *is the ability of the system to withstand an unwanted event* [43] – this is concerned with detecting and recovering from small defects before they can become larger failures
  - Checked at the verification stage
- Failure Tolerance requirements
  - Detailed in the main safety validation matrix – whereby software failure tolerance *concerns maintaining the system in a safe state despite a failure with the system* [43]
  - Checked at the verification stage

- Software Compliance – Evidence
  - Analysis evidence
  - Demonstration evidence
  - Quantitative evidence – in terms of the software standard DO-178B (and the withdrawn Def-Stan 00-55) the following quantitative values were provided for designers to prove the assurance of the software:

CPE Assurance Level	Failure Condition Classification	Design Assurance Level	Target Probability (per event for low usage system)	Target Probability (per flying hour)
High	Catastrophic	DAL A	10-5	10-9
Medium	Hazardous	DAL B	10-4	10-7
Low	Major	DAL C	10-3	10-5
Very Low	Minor	DAL D	10-2	10-3
Not Safety Related	Negligible	DAL E	N/A	N/A

Table 4: Software Quantitative Targets

- *Qualitative evidence*
- *Review evidence*
- *Process evidence*
- *Counter-evidence*

Software Safety

The software and complex hardware safety aspects form an important part of the analysis on top of the CPE certification (product and process assurance) efforts as the safety analysis should link the initial Functional Failure Path Analysis (FFPA) such as from FHAs down to the software FMEAs. Then after analysis during and after tests the functional flow paths from the S-FMEAs to the system level hazards (bottom-up approach) should be mapped. By doing this activity the safety requirements and hazard allocation (including risk budget) can be verified; any new hazards identified from the bottom-up analysis can then be included as a derived safety requirement and flowed back-up the analysis to determine whether the top targets can still be met. The following safety analysis should be undertaken:

- *Safety analysis*
  - *Software Fault Tree Analysis*
  - *Software FMECA (S-FMEAs)*
  - *Code Analysis and review*
  - *COTS and SOUP*
  - *Safety evidence and arguments*

Complex Hardware

Complex Hardware forms part of the CPE and the standards are contained in DO-254 [44]. The complex hardware devices can include Field Programmable Gate Arrays (FPGAs), Complex Programmable Logic Devices (CPLD) and Application Specific Integrated Circuits (ASICs). The general planning, V&V activities, configuration control, product & process assurance and safety analysis are also relevant but the electronic hardware philosophy is generally a top-down approach as this more effectively addresses safety design errors.

2.2.5 Accident Sequence

Once the safety definitions have been established (cause, hazard, accident, consequence) it is important to establish accident sequences as part of the analysis. Prior to discussing the accident sequence methods it is worth detailing the sequence in order to establish whether the current methodologies and definitions are sufficiently covered and more importantly sufficiently connected. The following figures represent basic accident sequences using the definitions from above:

Figure 10: Standard Accident Sequence

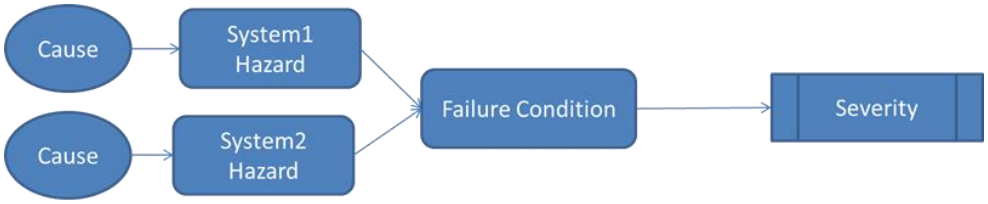


Figure 11: Failure Condition Sequence

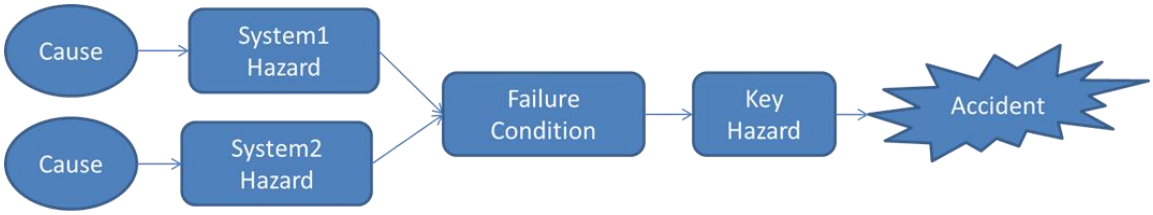


Figure 12: Modified Failure Condition Sequence to include explicit lower-level system hazard

As can be seen the figures are trying to tell the same story but are actually different. The point here is that hazard or accident or failure condition sequences can mean different things to different people and this is one of the reasons that the designer-oriented analysis is different from an operator-oriented analysis. This disconnect is discussed further in 3.4 whereby a more contiguous safety model is proposed incorporating the modified sequence and linking this to explicit aircraft-level hazardous states and then on to explicit accidents.

2.2.5.1 Tools & Techniques

The accident sequence can best be presented in Fault Trees and Event Trees:

Fault Tree Analysis

The following figure presents a typical and simple structure of a Fault Tree that shows how a base-event (cause) can lead through an intermediate event (hazard) and on to a top event (accident).

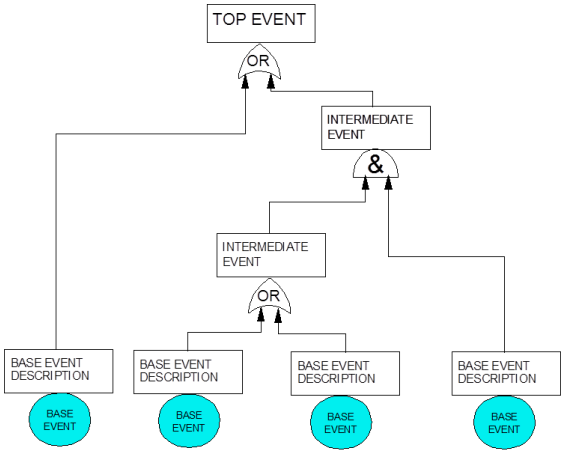


Figure 13: Basic Fault Tree Structure

FTA is a deductive technique i.e. ‘what causes this to happen’; it is a top-down analysis to determine the causes or base events. So we could start with the Accident ‘Loss of Control’ and say ‘what causes this to happen’ and we would then list those events. Next we would take those individual events and ask once again ‘what causes this to happen’ and so on until we get to the base events; these could be power supply failure, sensor failure, software failure and hardware failure. The FTA can ‘burrow’ a long way down to find a root cause and the boundaries of the analysis needs to be determined up front.

Event Tree Analysis

Figure 14 below presents a basic Event Tree showing an initiating event (this typically would be at the hazard level) and shows ‘developments’ (typically these would be controls) and leading on to final outcomes (accidents) and also consequences.

The ETA operates by forward logic from the question ‘what happens if?’ Here we follow logical sequences and we are determining the success or the failure of each event after the initiating event.

Although there are guidelines on how to use the separate tools as part of the overall safety effort, these are generally geared towards the Design Organisations. The DOs are responsible up to the failure condition in order to demonstrate compliance to a safety objective i.e. they can use FTAs

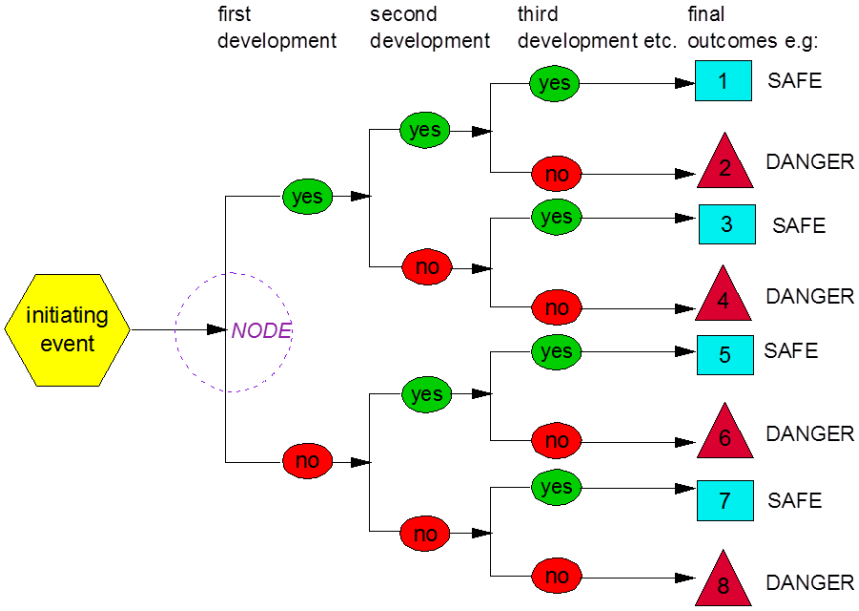


Figure 14: Basic Event Tree Structure

Another reason to understand the accident sequence is to be able to try and ‘break the chain’ to prevent the accident.

A slightly different approach used to identify the accident sequence is the ‘Loss Model’ technique. The Loss Model is another top-down deductive technique that uses qualitative analysis to demonstrate that the accident’s hazards and causes have been captured in a hierarchical manner. The Loss Model can be produced in readily available tools such as Microsoft Visio® as the model can be constructed in a simple fashion. The main point (as with all modelling of hazard and accident sequences) is to involve the right stakeholders i.e. subject matter experts; it is of little value to just have the safety engineer construct a Loss Model as he cannot know and understand the design and operation of every

system. Figure 15 depicts a simplistic Loss Model approach allowing the analyst to model a short path to the cause and even to include the cause control with the evidence detailed at the bottom.

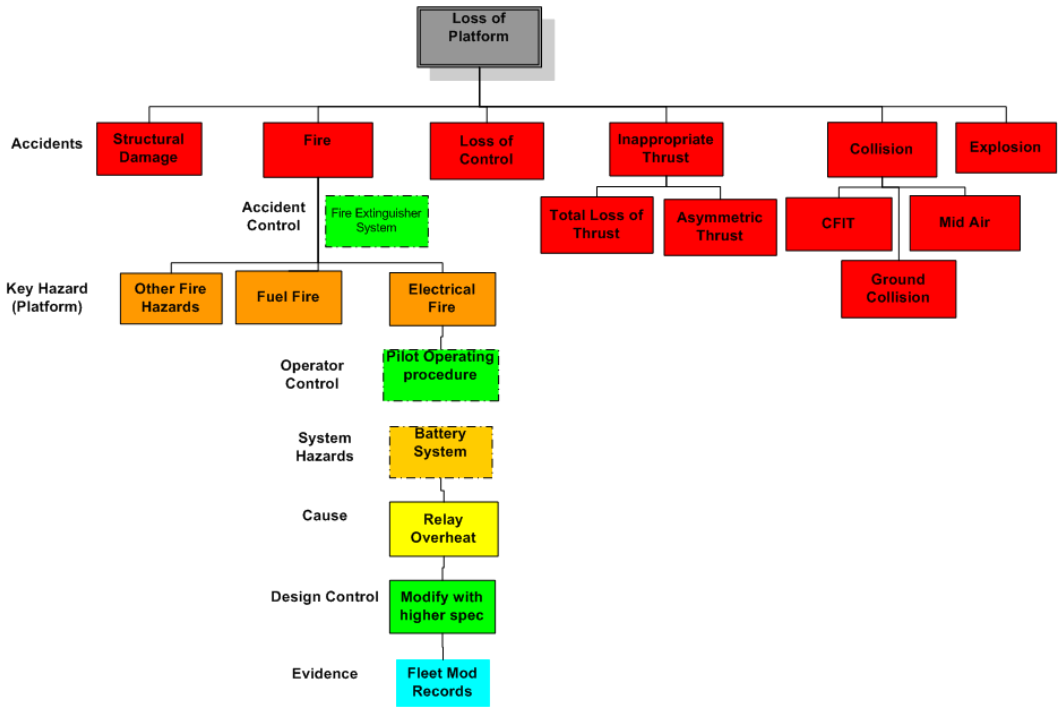


Figure 15: Simplistic Loss Model

Inherent Accident Sequences

Inherent hazard-to-accident sequences can be useful in addressing the non-technical aspects, such as 'slips and trips', exposure to lethal voltages and so on but the analysis also needs to address the operating and supporting of the equipment in order to ensure all hazards have been captured. As described above in Section 2.2.4 the OSHA activity is one method that addresses operating and support procedures from an Inherent sequence perspective. The OSHA model should provide a sequence of activities to analyse; it is up to the analyst how far back and how far forward he goes (from the actual flight) when analysing the procedures i.e. the analyst must define the scope of the OSHA model. In the generic 'Swiss-Cheese' model below the main defensive barriers are:

- Organisational Factors (manpower/resources/training)
- Procedures & Management
- Preconditions, Attitudes and Supervision
- Unsafe Act – this relates to the active decisions (i.e. managerial decisions to release an aircraft)/actions (i.e. pilot actions)

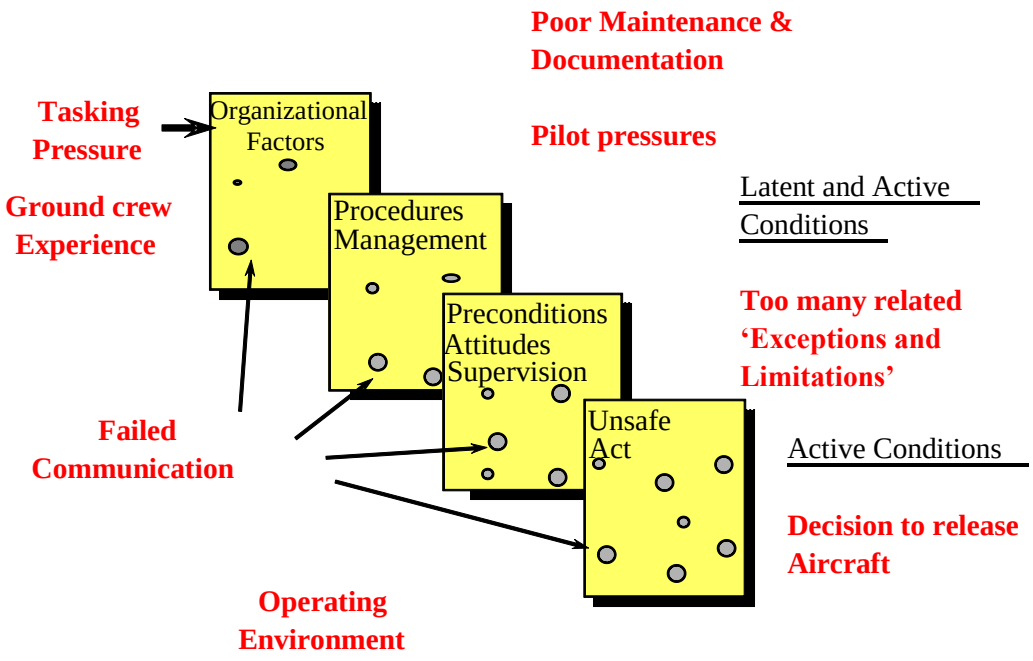


Figure 16: Accident Sequence Adapted from Reason's Swiss Cheese Model

As can be seen in the accident sequence above, 'failed communication' can be both a Latent issue and an Active condition on the day of the accident. Leverson [36] detailed these within her STAMP model as discussed in 2.2.6.4; there she suggests that the Socio-Political aspects play a factor in the total system i.e. regulators through to company executives through to the operators.

Operators need to understand the Inherent accident sequences just as much as the functional accident sequences as day to day the operators deal with Safety Significant Events and Inherent Accidents (as opposed to catastrophic accidents).

2.2.5.2 Accident Lists

Within DO and Operator safety analysis 'Accidents' are not explicitly considered within sequences. Instead DOs tend to analyse up to the Failure Conditions (which are associated with a severity i.e. catastrophic) and stop there. Operators tend to undertake reactive 'Risk Profiling' based on the Flight Operations Quality Assurance approach i.e. managing 'events' such as runway incursions or near fast landings.

In contrast, the military safety effort does focus on managing the Accident Risks but fails to manage the 'hazardous' incidents i.e. their severity classifications do not consider reduced safety margins (near mid-air collision, or near CFIT, etc.).

The ICAO SMS Manual [24] details recognised 'accidents' from the history of aviation occurrences. The Accident List is as follows:

- *Controlled Flight Into Terrain – CFIT*
- *Mid-Air Collision (MAC)*

- *Loss of Control – In flight (LOC-I)*
- *Loss of Control – Ground (LOC-G)*
- *Explosion (Fuel Related)*
- *Fire/Smoke (Non-Impact)*
- *Fire/Smoke (post impact)*
- *Loss of Thrust (system/component failure or malfunction – power-plant)*
- *Structural Failure*
- *System/Component failure or malfunction – non-power-plant*

ICAO standards also define 'Serious Incidents' which could also be used within a safety model (see Section 3.4):

- *A near collision requiring an avoidance manoeuvre, or when an avoiding manoeuvre would have been appropriate to avoid a collision or an unsafe situation (near MAC)*
- *Controlled flight into terrain (CFIT) only marginally avoided*
- *An aborted take-off on a closed or engaged runway, or a take-off from a runway with marginal separation from obstacle(s)*
- *A landing or attempted landing on a closed or engaged runway*
- *Gross failure to achieve predicted performance during take-off or initial climb*
- *All fires and smoke in the passenger compartment or in cargo compartments, or engine fires, even though such fires are extinguished with extinguishing agents*
- *Any events which required the emergency use of oxygen by the flight crew*
- *Aircraft structural failure or engine disintegration which is not classified as an accident*
- *Multiple malfunctions of one or more aircraft systems that seriously affect the operation of the aircraft*
- *Any case of flight crew incapacitation in flight*
- *Any fuel state which would require the declaration of an emergency by the pilot*
- *Take-off or landing incidents, such as undershooting, overrunning or running off the side of runways*
- *System failures, weather phenomena, operation outside the approved flight envelope or other occurrences which could have caused difficulties controlling the aircraft*
- *Failure of more than one system in a redundancy system which is mandatory for flight guidance and navigation*

These ICAO-based taxonomies are useful to use within the accident sequence and they can explicitly link to corresponding failure conditions and other contributory factors. This is explored more in Chapter 3.4.

Inherent, people-based Accidents are more difficult to assign in terms of the aircraft/spacecraft analysis as this is not well documented. In order to manage the Total System Risk (discussed more in 3.4.11) DOs should analyse the operating and support aspects during the development of the aircraft but they should do this with the Operator. It is only by undertaking a joint analysis will both 'sides' understand and be able to manage the inherent hazards (and accident risks) associated with the platform. An example would be a 'slip & trip' **hazard** that is **caused** by a large centre-console design in a small cockpit that leads to a Musculoskeletal **Accident** with the **consequence** of severe cut or bruise. Another example is 'exposure to lethal voltages' **hazard** that is **caused** by poor bonding/earth

termination leading to an Electrocution **Accident** with the **consequence** of death[10]. So it is also important to establish proper sequences with Accidents such that hazards can be linked to them and 'accident controls' implemented. Clearly the DO can address the root causes (such as the poor bonding or improve the centre-console design) but the Operator can then implement operating procedural controls, warning signs or limitations.

Even within the Health & Safety documentations and references there is confusion in that they talk about accidents but then go on to say that:

> *'For slip and trip risks to be adequately controlled you need to undertake a risk assessment'*[11] *and:*
>
> *'Many slip, trip and fall accidents occur on the ground in the UK where existing UK Health and Safety legislation applies - Hazards associated with slips, trips and falls in the aircraft cabin and flight deck environments include …. Stairwells, open aircraft exits, etc.'*[12]

As can be seen the first example talks about the risk of a slip or trip and the second example talks about the slip or trip being an accident with the hazard being stairwells, open aircraft doors and so on; here it is considered that the hazards are actually causes and that the slip and trip is not an accident. It is also understood that 'one man's hazard is another man's cause and this confusion is believed to be rooted in the fact that Accident Lists are not generated or used within the safety domain – even though ICAO have accident lists.

2.2.6 Risk Management

(Safety) Risk Management is the core safety activity that underpins the robustness of a safety case. It is important to define Risk (and Risk Management) because it is the author's considered opinion that there is confusion between DOs and Operators as to the difference between a hazard assessment and a risk assessment:

Risk Definitions

- Def-Stan 00-56 [28]; *Combination of the likelihood of harm and the severity of that harm*
- FAA-AST AC [18]; *Measure that takes into consideration the likelihood if occurrence and the consequence of a hazard to people or property*
- ANSI [84]; *a measure of the expected loss from a given hazard or group of hazards. Risk is a combined expression of loss severity and probability (or likelihood). When expressed quantitatively, risk is the simple numerical product of severity of loss and the probability that loss will occur at that severity level*.

Risk Management Definitions:

- Def-Stan 00-56 [28]; *The systematic application of management policies,*

---

[10] The terms 'musculoskeletal' and 'electrocution' are detailed here as the 'accident' within a sequence. It is difficult to name this event (the accident) with inherent events as it is easy to confuse the event as a hazard or even the consequence, so care must be exercised when trying to establish inherent-based sequences. The European Agency for Safety and Health at Work[10] details various disorders such as Musculoskeletal Disorder which covers aspects (hazards) including Noise, Vibration and Manual Handling.

[11] http://www.hse.gov.uk/slips/employersriskas.htm

[12] http://www.caa.co.uk/docs/33/cap757.pdf

procedures and practices to the tasks of Hazard Identification, Hazard Analysis, Risk Estimation, Risk and ALARP Evaluation, Risk Reduction and Risk Acceptance.

- FAA-AST AC [18]; 'Risk Mitigation' *is a process of reducing the likelihood of occurrence, severity of occurrence, or both the likelihood and severity of a hazard to people or property*.
- ANSI - none

By undertaking Risk Management an Operator can determine whether a Total System can be deemed 'Acceptably Safe'. Here it is meant that the operator has taken an aircraft (or suborbital aircraft) that has met its design airworthiness criteria (failure condition safety objectives) and applied their operator procedures and limitations and have assessed the individual accident risks and then assessed the cumulative risks to the aircraft and derived this to be acceptably safe.

'Safe' is described in the UK Defence Standards [28] as:

> *"Risk has been demonstrated to have been reduced to a level that is ALARP and broadly acceptable, or tolerable, and relevant prescriptive safety requirements have been met, for a system in a given application in a given operating environment."*

Therefore the term 'acceptably safe' as applied to a suborbital aircraft is derived as:

- The Risk to a suborbital aircraft has been demonstrated to have been reduced so far as is reasonably practicable and that relevant prescriptive safety targets and safety requirements have been met for all phases of the suborbital flight

To demonstrate a safe System, Design Organisations (and Operators alike) will identify Safety Requirements that must be met. Safety Requirements are defined in the UK Defence Standards [28] as:

> *"Specified criteria of a system that is necessary in order to reduce the risk of an accident or incident to an acceptable level. Also a requirement that helps or achieve a Safety Objective"*

As part of the Safety Requirements it is also important to have robust safety criteria to which a DO must meet.

2.2.6.1 Safety Criteria & Targets

Civilian Airworthiness Codes of Requirements

The Aircraft Loss Target stated in Federal Aviation Regulations (FAR)/Certification Specification (CS) 25.1309 [87] is based on the world-wide accident rate which is about one per million flight hours, i.e. a probability of 1E-6 per hour of flight. The accident rate was first analysed in the UK for the British Civil Aviation Requirements (BCAR). It was deduced that the baseline rate was due operational and airframe related causes. Furthermore about 10% of accidents were attributed to failure conditions involving critical aircraft systems, i.e. 1E-1; therefore the overall target should be no greater than 1E-7. Arbitrarily it was deduced that there were approximately 100 system catastrophic failure conditions assumed to exist on civil aircraft, i.e. 1E+2. Therefore to prevent a deterioration of the current fatal accident rate, DOs must show that the probability of occurrence of each catastrophic failure condition was at least 1E-6 x 1E-1 / 1E+2 = 1E-9 per flying hour. This then became the basis for inclusion in the relevant Certification Specification's codes of requirements for designing aircraft.

AC 25.1309-1A [51] details the acceptable means of compliance for § 25.1309(b) and of particular relevance is the 'probability versus consequence' graph. The probability classifications based on the above rationale are as follows:

- *Probable failure conditions > 1E-5*
- *Improbable failure conditions <1E-5 but > 1E-9*
- *Extremely Improbable failure conditions <1E-9*

The AC states that each failure condition should have a probability that is inversely related to its severity. It is recognised that should the Designer present an aircraft with 100 catastrophic failure conditions that meet the safety objective of 1E-, then they will meet the overall Loss Target (for catastrophic failure conditions) of 1E-7. §25.1309 then stipulated further safety objectives: Major failure conditions are to be <1E-5 and >1E-9 and Minor failure conditions >1E-5; therefore one would assume that with a further 100 'Major' failure conditions met by the DO at 1E-5 then they will meet that overall target of 1E-03.

The range of the Major failure conditions is clearly too great, hence the FAA tasked the Aviation Rulemaking Advisory Committee (ARAC) with providing better guidance for DOs to follow. Their report [46] includes an updated AC 25.1309 and quite rightly splits the 'Major' failure condition criterion to the following classifications (severity/ probability):

- *No Safety effect/no probability requirement*
- *Minor/Probable failure conditions < 1E-3*
- *Major/Remote failure conditions <1E-5*
- *Hazardous/Extremely Remote failure conditions <1E-7*
- *Catastrophic/ Extremely Improbable failure conditions <1E-9*

One question to ask with the chosen category ranges is why there are two orders of magnitude between the severity classifications (base 100) as opposed to a logarithmic scale using base 10 (and also why there were four orders of magnitude beforehand)? In answering this we must first look at the probability definitions:

- Extremely Improbable Failure Condition: a failure condition that is so unlikely that it is not anticipated to occur during the entire operational life of all airplanes of one type.

  Note: This probability *includes a fail-safe design requirement that single failures must not result in catastrophic failure conditions, regardless of their probability*.

- Catastrophic Failure Condition: a failure condition that would result in **multiple fatalities**, usually with the loss of the airplane.

The multiple fatalities for catastrophic could refer to 100 people (as a rough order in a large passenger aircraft) and therefore the severity ranges per probability range reduce by two orders of magnitude i.e. by 100. Following this argument would mean that Hazardous events result in 1 death or 100 severe injuries and Major events result in 100 slight injuries. This rationale concerns looking at the harm (consequence) from the severity of the failure condition and therefore considers the risk of the accident; this is different from the risk of the failure condition. Furthermore this rationale does not consider that the original AC25.1309-1A [51] suggested four orders of magnitude between failure conditions.

In the UK Military Risk Matrices base 10 is used in a logarithmic scale but there is no explanation as to why; the military have small fast jets and helicopters with less than 10 people on board but also have large transport aircraft – if this were the case then there should be two Risk Matrices.

It is therefore more credible that the probability ranges stem from the origins of the catastrophic failure condition (1x10-9 per flying hour for Part 25 aircraft and commuter category aircraft in Part 23) and that the reducing severities and associated probabilities were derived from engineering judgment. This is further backed up by the use of phrases such as '*because the improbable range is broad, the applicant should obtain early concurrence of the cognisant certificating office on an acceptable probability for each major failure condition'* [51]. Furthermore the original AC states that due to the fact that failure rate data is not precise that there is a degree of uncertainty (as indicated by the **wide line** on Figure 17 below) and that the descriptive probability expressions stated '*on the order of'*.

This revised probability scheme has been incorporated in CS 25 [48]. The consequence versus probability graph is still a single safety objective/overall target line; the axis has changed i.e. probability on the vertical axis, and they have explicitly added the words 'unacceptable' above the safety objective line and 'acceptable' below. By keeping with the single line philosophy, this means that there is still an implicit 'overall target' for each type of failure condition (catastrophic/ hazardous/major/minor) as depicted in Figure 17 below.

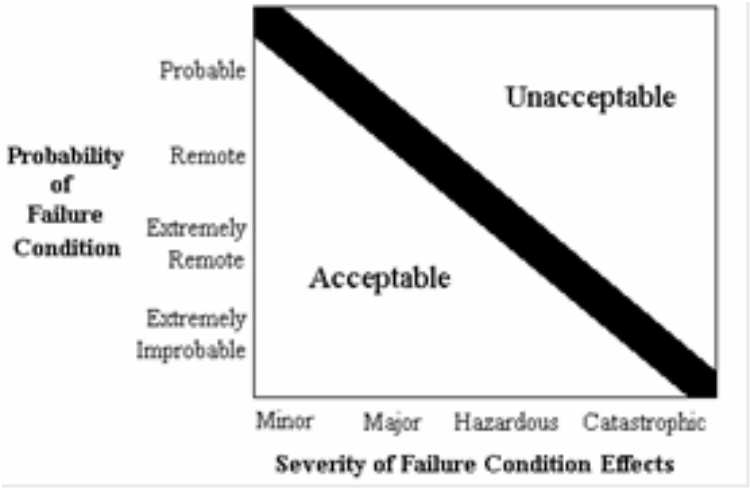


Figure 17: AC 25.1309 severity and probability criterion

Recognising that smaller aircraft will have different characteristics than large aircraft a certification specification (CS) and AC were introduced. CS 23 [47] covers Normal, Utility, Aerobatic and Commuter Category airplanes. It details the applicability and provides a breakdown of categories of aircraft stating that an aircraft can be certified under more than one category so long as it meets all of the relevant and identified requirements. AC 23.1309 [87] follows the same rationale as §25.1309 with the aim as:

> *'to improve the safety of the airplane fleet by fostering the incorporation of both new technologies that address pilot error and weather related accidents and those technologies that can be certificated affordably under 14 CFR Part 23'*

Although the AC covers all of the categories stated above, it concentrates on the General Aviation (GA) aspects in rationalising the decision regarding the setting of safety objectives. The historical accident rate is predominantly associated with flying in Instrument Meteorological Conditions (IMC). The evidence indicates that the probability of a fatal accident in restricted visibility due to operational and airframe-related causes is 1 in 10,000 (1E-4) for single-engine aeroplanes under 6000lbs. Additionally (as per §25.1309) evidence shows that 10% of accidents are due to system failure conditions therefore the probability of a fatal accident from all causes is 1E-5 per flight hour. As opposed to large aircraft with many complex systems, Part 23 Class I aircraft are 'arbitrarily' derived to have 10 potential failure conditions that could be catastrophic thus the safety objective is 1E-6 per flying hour. The AC continues to state that larger aircraft (than Class I) have a lower failure rate and therefore have lower probability values for catastrophic failure conditions:

- *Class II = 1E-7*
- *Class III = 1E-8*
- *Class IV = 1E-9*

Although there is no 'severity versus likelihood' chart as per §25.1309, the chart would be exactly the same as in Figure 17 above.

Airworthiness for Protection

The codes of requirements are detailed for the assurance of the airworthiness of the aircraft in accordance with ICAO Annex 8 [49], where the foreword states:

> *"The objective of international airworthiness Standards is to define..... the minimum level of airworthiness...for the recognition...of certificates of airworthiness... thereby achieving, among other things, protection of other aircraft, third parties and property"*

This overarching statement considers the aircraft, 3rd parties and property. Implicit in the *aircraft* part of the statement is clearly the crew (1st parties) and passengers (2nd parties); though CS's and other requirements have more explicit requirements concerning safety of passengers and crew.

Military Safety Targets

UK Military

The UK Military have adopted a top-down 'Safety Target' approach for all of their aircraft [50]. The Safety Target is detailed as:

'the cumulative probability of the loss of an aircraft due to a technical fault and the cumulative probability of a technical failure of the aircraft (inclusive of its systems, structure and stores) which could result in the death of any air crew or passengers, should both be assessed to be of the order of one in a million per flying hour (probability of occurrence **$1x10^{-6}$ per flying hour**) when operated within the conditions used for the airworthiness demonstration'

This then is not prescriptive in its use of safety objectives for failure conditions (or hazards) and does not detail the number of 'arbitrary' safety critical failure conditions i.e. it does not state that there are 100 catastrophic failure conditions; nor does it detail the 10% attributed to operational and airframe related causes. It is recognised within the military that this safety target was mainly introduced to provide a goal for aircraft already 'In-Service'. For newly contracted aircraft, this safety target was the only contracted requirement and therefore Designers were left to their own conclusions in the

derivation of safety objectives for failure conditions i.e. were they contracted to 1E-8 or 1E-9 per flying hour for catastrophic failures?

It is also recognised within the military that the safety target includes a mixture of design controls, operating procedural controls and limitations (these latter aspects covered within an aircraft's Release to Service).

Also it is clear from within the safety target statement that the military explicitly considers the crew and passengers in their criteria, but not 3rd parties or property; these are implicit requirements and 3rd parties in particular are covered within the severity classifications (property is not).

The risk matrix and criterion used by the standard UK military Project Team is as follows:

	Catastrophic	Critical	Marginal	Negligible
Frequent **(>10-3)**	A1	A3	A7	B13
Probable **(10-3 to 10-4)**	A2	A5	B9	C16
Occasional **(10-4 to 10-5)**	A4	B6	C11	C18
Remote **(10-5 to 10-6)**	B8	C10	C14	D19
Improbable **(10-6 to 10-7)**	C12	C15	D17	D20
Incredible **(<10-7)**	D21	D22	D23	D24

Table 5: UK Military Aviation Standard Risk Matrix

As can be seen above the Project Team's tend to use this for Accidents and Hazards with some filling in the table using Hazard Risk Indices (HRI) similar to that in Table 6 below. However the military guidelines do not explain the derivation of the numbers and how Project Teams were supposed to use them, other than one could differentiate between a high 'C' and a low 'C' Risk in the critical, marginal and negligible columns (likewise for the other A and D class cells) i.e. the 'risk' is a C10 so you know where this sits in the matrix. However this approach seems to be a mix of accident risk criterion (using Risk Class A, B, C and D) as well as a HRI scheme (1-24); though the cell values start at 1 (for catastrophic/frequent) and apart from identification purposes there is no rationale and no correlation to number of hazards per severity classification per the explicitly defined US system below.

In summary there is much confusion with the way the UK Project Teams use their Risk Matrix (as well as the accompanying probability and severity classifications) and the newly installed UK Military Aviation Authority intend to revamp the criterion and are looking towards civilian best practices to be applied to new military aircraft developments.

US Military

The US military tend to follow the MIL-STD-882 [53] guidelines and also the Joint Service Specification Guide (JSSG) for Air Vehicles [52]. The later was produced to support '*performance-based aviation acquisition'*. The JSSG provides useful insight into the derivation of Hazard Risk Indices (HRI) and the following table shows one form of using HRIs during the development stage

when setting requirements. The HRIs are derived from multiplying the values associated with the frequency and consequence i.e. Frequent (6) x Catastrophic (5) = 30 and so:

	Hazard Frequency					
Hazard Consequence	Frequent	Probable	Occasional	Unlikely	Remote	Improbable
Catastrophic	30	25	20	15	10	5
Critical	24	20	16	12	8	4
Significant	18	15	12	9	6	3
Marginal	12	10	8	6	4	2
Negligible	6	5	4	3	2	1

Table 6: JSSG exemplar Hazard Risk Indices Table for aircraft procurement

The extremely useful concept of numbering the matrix this way is that it links in to the origins of the failure conditions in that it appreciates where the *$1x10^{-9}$ per flying hour* stems from (which includes an arbitrary 100 hazards). In the above table it is assumed that there are 100 hazards and that the cumulative value for catastrophic failures is 1000, then for development if there are 33 hazards that are catastrophic/frequent that the 'target' will not be met. Additionally the guide suggests that the risk matrix can be 'calibrated' by having a '*forbidden zone'* and following the same regime as before this value is entered as 1001 and in the example below the forbidden zones are the high frequency, high consequence area:

	Hazard Frequency					
Hazard Consequence	Frequent	Probable	Occasional	Unlikely	Remote	Improbable
Catastrophic	1001	1001	20	15	10	5
Critical	1001	1001	16	12	8	4
Significant	18	15	12	9	6	3
Marginal	12	10	8	6	4	2
Negligible	6	5	4	3	2	1

Table 7: JSSG exemplar Hazard Risk Indices Table including 'forbidden zone'

In the above example an aircraft designer could have the following number of catastrophic 'hazards'; 30 (occasional), 20 (unlikely) and 10 (remote) – the guide suggests that hazards equal to or less than those in the 'blue zone' are not counted in the cumulative calculation and so the remaining 40 hazards must be within the Improbable cell.

This methodology is explicit in its rationale and this is encouraging because in reviewing other documents it is not clear sometimes how they have derived their criteria or risk matrices (whether hazard based or accident based).

Abort Rate Methodology

Another method of deriving a platform Loss Rate was discussed by Reaction Engines at the 2nd IAA conference [54]. The rationale for the choice of an abort rate was that the 'space-plane' industry cannot afford the flight test criteria afforded by aerospace design and manufacture whereby the development costs would be recuperated by mass sales. Although a lot of evidence would be gathered

by design analysis and computer modelling and wind-tunnel testing of sub-scale models the actual flight tests (for Reaction Engines) was stated to be 300 between two prototype vehicles with a further 76 flights in reserve. Their space vehicle 'SKYLON' is designed for orbital operations though the methodology is considered here as an alternative to the normal certification criteria which is based on well-proven systems. Their methodology was as follows:

- *Assumes link between Abort Rate and Loss Rate*
- *Assumes 2 abort events would lead to Loss*
- *Assumes 50% crew survivability in aborts*

Therefore probability of fatalities is half the probability of airframe loss =

$$\mathbf{P_{fatal} = P_{loss}/2} \qquad \textbf{[}\textit{Equation 1}\textbf{]}$$

Therefore Probability of loss is dependent over time [P (t)] whereby $P_{abort} = \int P(t)$ and for two aborts this means that after the first abort the probability function for the second abort is half therefore;

$$\mathbf{P_{loss} = \int P(t) * \int P(t) /2 = P_{abort}{}^2/2 \text{ therefore,}}$$

$$\mathbf{P_{loss} = P_{abort}{}^2/2} \qquad \textbf{[}\textit{Equation 2}\textbf{]}$$

Thus combined with Equation 1, the result is the estimated probability of fatality =

$$\mathbf{P_{fatal} = (P_{abort}{}^2/2) / 2 = P_{abort}{}^2 / 4} \ \textbf{[}\textit{Equation 3}\textbf{]}$$

With a 1/100 abort rate (after 300 flights) this implies a vehicle loss rate of 1 in 20,000 which equates to a loss of life probability of 1 in 40,000 and therefore they claim that their initial estimates suggest they are more than one hundred times 'safer' than the Space Shuttle.

They then suggest that a rolling certification program could be achievable to prove 1 in 10,000 (1.0×10^{-4} pfh) by showing an abort rate of 1 in 225 (300 flights with no aborts or 500-1000 flights to establish a probability function). Then moving to 'approach 2' whereby they prove 1 in 1,000,000 (1.0×10^{-6} pfh) by showing an abort rate of 1 in 700 (1000 flights with no abort or 3000 to 4000 flights to establish a probability function).

This methodology of linking an abort rate to the loss rate is an interesting approach and needs to be further analysed as to the suitability for aircraft-based vehicles; it is considered this may be an appropriate method for vertical take-off/vertical landing vehicles in the suborbital domain; this suggestion is captured as a recommendation in 6.4.

Conclusions on Safety Criteria & Targets

Parts 23.1309 and 25.1309 baseline criteria are based on historical accident rates for the type (size) of aircraft. The levels of safety objectives for the failure conditions are then derived accordingly from codes of requirements and these are solely for the Design Organisation to demonstrate their compliance to as part of the certification process. These baseline criteria (and subsequent derivation of safety objectives) use sound methodology and for the suborbital field the same methodology could be employed (for aircraft-based vehicles); however it is clear that the baseline criterion must first be established, ensuring that the rationale is explicit and relevant. It was evident from the review that some criteria was not rationalised and this causes confusion (in particular in the UK military airworthiness and safety domain).

In terms of a 'Safety Target' approach, this does not fit into the existing civilian methodology, but there may be merit in adopting a combined approach because for suborbital vehicles (and in particular

for the rocket engine) the civilian safety objectives (such as 1E-8 pfh) may be extremely difficult to achieve without some credit taken from operating procedures or limitations. Additionally, it may be more prudent to explicitly detail the consequences to 1st, 2nd and 3rd parties (and property) within the classifications. This aspect is further discussed in Chapter 3.

The alternative method of calculating an abort rate and linking it to a loss rate is an interesting approach and one that may suit suborbital vertical take-off and landing vehicles in particular.

Final Views on Risk Assessment and Risk Matrices

This section has shown that there are various methods in assessing hazards (failure conditions) and accidents and sometimes these get mixed up. The author contends that there should be a clear distinction between **functional analysis** for certification of aircraft (and in EASA terms a certified aircraft implies that the flight crew and passengers are safe and so are those that are overflown by the aircraft) and **inherent people-based analysis** whereby risks to individuals or groups of people (pilots, maintainers, passengers and the public etc.) can be analysed and risk reduction carried out (to ALARP for instance as in the UK); for functional aircraft analysis the metric is 'flying hours' and for people-based analysis the metric is 'risk per person (per group) per year'. Additionally the author contends that it is acceptable to analyse individual risks to determine whether further risk reduction is required but that these individual risks (r) must then be aggregated to provide a cumulative risk i.e. Total Risk (R); this could be per severity or indeed for all risks. Therefore when compiling Risk Matrices the metric should be clear as to whether they represent a hazard or accident and whether they represent flying hours or risk to people. When summing the risks or analysing them individually care must be taken so as to apply the correct disproportion factor at the correct level (in the UK ALARP calculation in particular); otherwise the risk may be falsely presented leading to incorrect decisions being made as to whether to apply a risk reduction measure. Finally the Risk Matrices are sometimes not logarithmic or indeed not plotted per convention i.e. a Cartesian plot whereby severity is conventionally plotted increasing left to right on the x-axis and likelihood increasing vertically on the y-axis.

2.2.6.2 Risk Estimation

Risk Estimation determines (quantitatively or qualitatively) the risk consequences of individual Accidents; this takes into account the relevant hazard-to-accident sequences and in particular those hazards that are the main contributors to the Accident.

Preliminary Risk Estimation (PRE) takes the Risk Estimation and attempts to classify the Risk of each Accident in terms of the 'confidence' level of the Risk presented. Once the PRE process has been completed the Risks can then be prioritised in order (highest to lowest) so that the most serious risks are looked at first when undertaking the Risk & ALARP Evaluation process. As well as estimating the Risk, the PRE process is one method of determining whether a project is viable in terms of meeting safety objectives/targets whether at the failure condition (system) level or the accident risk (platform) level.

2.2.6.3 Risk & ALARP Evaluation

The As Low As Reasonably Practicable (ALARP) principle stems from the UK Health & Safety Executive (HSE) definitions. The UK Defence Standards and others have taken the definitions and used them within their own standards:

- UK HSE definition [55]:

At the core of ALARP is the concept of 'reasonably practicable' which involves weighing the risk against the trouble, time and money to control it. Thus ALARP describes the level to which it is expected that workplace risks are controlled to.

- UK DEF-STAN 00-56 [28]:

A risk is ALARP when it has been demonstrated that the cost of any further Risk Reduction, where the loss of (defence) capability as well as financial or other resource cost, is grossly disproportionate to the benefit obtained from the Risk Reduction.

- ANSI [84]:

That level of risk which can be further lowered only by an increment in resource expenditure that cannot be justified by the resulting decrement in risk. Often identified or verified by formal or subjective application of cost-benefit analysis or multi-attribute utility theory.

In terms of the above definitions there is a different emphasis from the HSE description of ALARP to that of the UK Defence Standards and also the American National Standards. In the latter the intent is that the Risk is applied towards military equipment (primarily in the air domain which concerns functional and inherent hazards [and their probabilities in flying hours] associated with a particular accident risk [factor of severity and the probability]). In the UK HSE domain the intent is to identify risks in the workplace and classify them in terms of tolerability towards the societal perspective; to do this the risk is deemed in terms of the risk to the population (of workforce or group) per 100,000 people per year i.e. the risk is measured in terms of risk per person per year (pppy).

The following 'ALARP Triangle' represents the degrees of risk in terms of acceptable deaths per person per year (per societal group) and is adapted from the HSE's Reducing Risk Protecting People (R2P2) [56] guidelines:

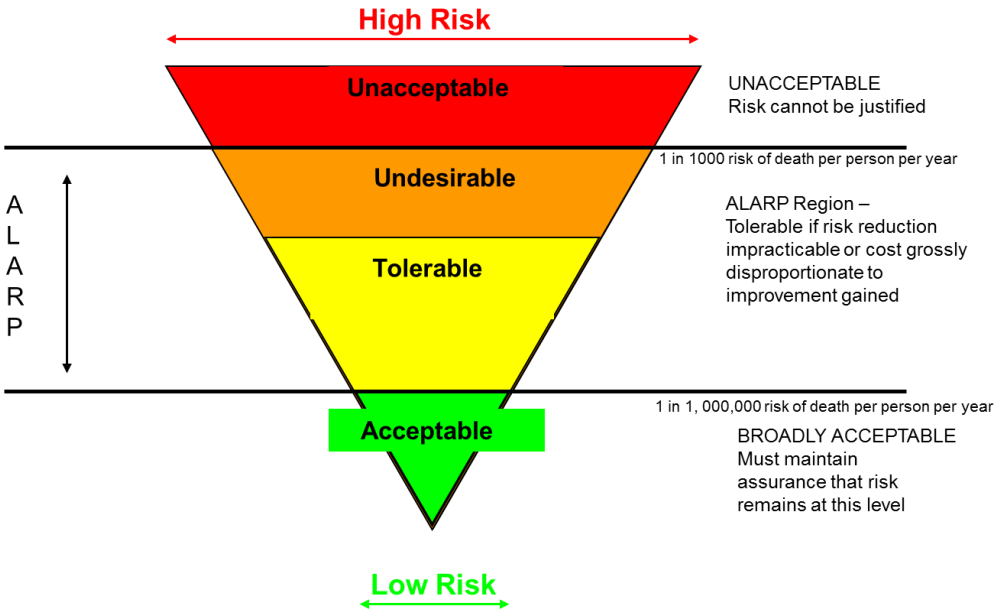


Figure 18: HSE – based ALARP Triangle depicting Tolerability of Risk

It is considered that the UK military have adapted the basis of the ALARP principle and applied this to the airworthiness (certification and safety risks) aspects. The Project Teams base their analysis on the flying hour rates and do not consider risk of death 'pppy'. Chapter 3.4.9 provides a more explicit method to address the issue of flying hour 'versus' risk of death pppy.

In demonstrating ALARP the UK HSE suggest that duty holders can do this by arguing risks are reduced to ALARP by following the order of precedence below:

- *Good Practice; here a duty holder can argue that he has followed good practice in implementing various levels of controls*
- *Qualitatively; here a duty holder may argue engineering judgment and common sense in the approach*
- *Quantitatively; in this instance more formal methods may be required to argue that the risk has been reduced to ALARP. This may include quantitative assessment backed up by a Cost Benefit Analysis (CBA) to demonstrate that the benefit gained from introducing a control measure is commensurate to the costs involved in the design, development and through-life management of the control*.

As can be seen in the UK Def-Stan 00-56 definition further above that the CBA effort provides a clear indication whether the cost of a control measure is *grossly disproportionate* to the benefit gained in which case the duty holder can argue against the implementation of said control; likewise if the cost is less than the calculated 'ALARP Budget' then the duty holder should implement the control. An example of this is provided in 4.2.

2.2.6.4 Risk Reduction

To demonstrate that risks are ALARP one has to state and justify the existing controls are actually implemented and are effective. The next stage is to identify additional potential controls to reduce the risk. Then the potential controls can be subject to an optimisation analysis to determine which of the controls should be implemented. This can then be documented as part of the safety justification that determines the risk is ALARP and is ready for the next phase of risk acceptance (2.2.6.5).

Risk Reduction is the key component within an accident sequence because it is the one variable that we can have more of an influence on than for example the direct root cause. Many factors can have an influencing effect on the accident sequence including; the management, the media (environment), man (the human factor) and the machine and these can clearly be articulated in the 5-M model (2.2.8).

Leverson [36] describes the many factors within a Socio-Technical based model called STAMP (Systems-Theoretic Accident Model) which suggests that *accidents occur when external disturbances, component failures, or dysfunctional interactions among systems are not adequately handled by the controls system, that is, they result from an inadequate control or enforcement of safety-related constraints on the development, design and operation of the system*. Within the paper her model focuses on the *hierarchy of control based on adaptive feedback mechanisms* and this is applied to the 'whole system' meaning the total Socio-Technical aspects including legislation, regulations, certification, and design systems safety through to the operator safety. The model then refines the failure of controls (constraints) to three high-level *control flaw classifications*:

- *Inadequate Enforcement of Constraints (Control Actions)*
- *Inadequate Execution of Control Action*
- *Inadequate or missing feedback*

In the systems theory part of the model Leverson with regards to the *hierarchy of control based on adaptive feedback mechanisms* she cites a paper (Ashby, 1956) that states *that to affect control over a system requires four conditions*:

- *The controller must have a goal or goals (e.g., to maintain the set point)*
- *The controller must be able to affect the state of the system*
- *The controller must be (or contain) a model of the system, and*
- *The controller must be able to ascertain the state of the system*

The above control laws pertain to both humans and the automated system and can act independently or may act together i.e. in terms of modelling this within a Fault Tree the former would be either the human OR the automated system providing a control or in the latter case the human AND the automated system provides the control. Figure 19 below depicts the human and automated control systems and when explicitly shown like this provides a clear picture of why the human control may fail, in that due to the human factor aspects the human's model of either the controlled process or the automated model may become flawed.

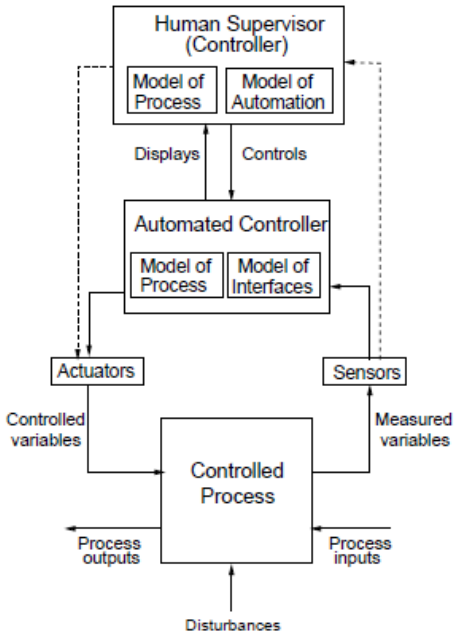


Figure 19: A typical control loop and process model (from Leverson's STAMP model)

Some of these human factor aspects are discussed in the 5-M model (2.2.8) but to continue the analyses of these flaws (or variability in performance) we turn to another approach based on the Functional Resonance Accident Model (FRAM) by Hollnagel. A paper on Resilience Engineering and Safety Management Systems in Aviation by Dijkstra [37] depicts the model (FRAM, Hollnagel 2004) and suggests the use of the model requires performance indicators.

The FRAM essentially re-classifies failures and 'errors' to variability in performance and encompasses an alternative approach to capture the *dynamic nature of how events occur*; to use *resonance rather than failure*.

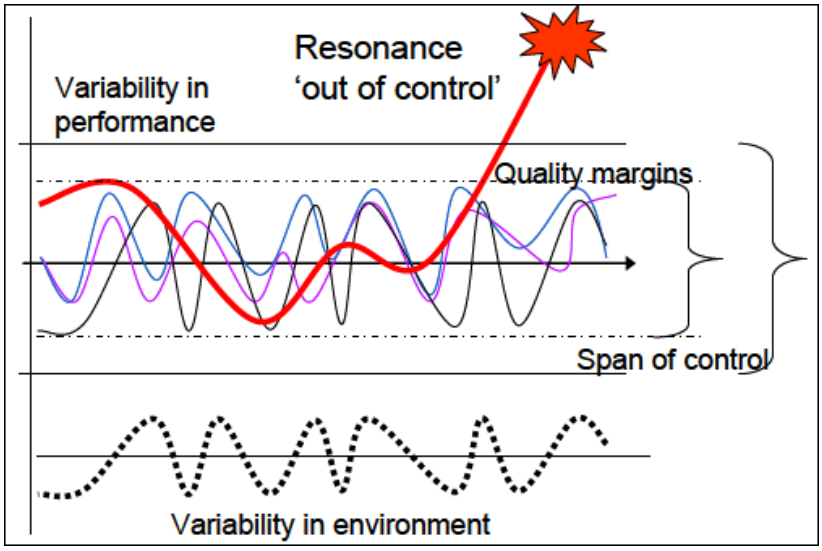


Figure 20: Functional Resonance Accident Model

In the model the variability in performance reflects the performance of the system where the human and machine form part of that system. This model is an interesting concept whereby the 'quality margins' of the resonance can be pre-set values and for the automated system this is already the case whereby a warning or alarm is provided, however for the human these quality margins also need to be set; these margins of human error are discussed in 2.2.8 and refined into guidelines at 3.4.6.

2.2.6.5 Risk Acceptance

Risk Acceptance is the final stage in the RM process. Once all of the previous RM activities have been completed, the Risk Acceptance process should address how the sufficiency and adequacy of the supporting evidence will demonstrate that the Risk is Acceptable. The HSE classify the risks as:

- *Unacceptable*
- *Tolerable*
- *Broadly Acceptable*

Within the UK MoD an additional layer of tolerability is introduced. Risks are either:

- *Unacceptable*
- *Intolerable*
- *Tolerable*
- *Broadly Acceptable*

The FAA-AST AS [18] has introduced a simplified risk acceptability matrix whereby they have two categories:

- *Category 1 – High (1-6, 8 – in terms of Hazard Risk Index [HRI])*
- *Category 2 – Low (7, 9-20)*

The ANSI [84]; mishap risk categories are:

- *High (1-5)*
- *Serious (6-9)*
- *Medium (10-17)*
- *Low (18-20)*

The tolerability criteria detailed above are similar in their methods by having a ‘medium’ or ‘tolerable’ area whereby accountable decision makers can accept (or not) the risks presented to them (except the FAA-AST guidelines for commercial spaceflight – where the risk is simply acceptable or not).

2.2.7 The Hazard Log

The Hazard Log is the cornerstone of a safety case and if structured correctly can provide a useful and auditable source of evidence. The ICAO SMS Manual [24] states that a hazard log should:

- *Record hazards*
- *Have hazards with unique assigned numbers*
- *Describe each hazard*
- *Detail the consequences*
- *Assess the likelihood and severity of the Safety Risks*
- *Detail safety risk controls (mitigation measures)*
- *Be updated for new hazards and safety risk controls*

The hazard log is an extremely powerful tool if used correctly and during the author’s visits to the safety offices of two airlines it was evident that the hazard log was an aspiration rather than a tool being used to determine the airline’s Safety Risk. Instead the preferred method was to use Risk Profiles based on the Flight Operations and Quality Assurance (FOQA) model. This takes individual occurrences and records them so that one can display the rate of occurrences in a Risk Profile. Once this is achieved it is easy to see what the airline’s issues are i.e. runway incursion, high speed/angle approaches due poor Air Traffic ‘let-downs’ and also inherent issues such as ‘Despatcher falling from aircraft steps’. These however are based on the *frequency* of the occurrence only and the Safety Manager may spend time on undertaking Risk Assessment for these issues whereas their highest Risk may actually be on a lower event in the Risk Profile; hence they need to include *severity* in their Risk Profile charts i.e. displaying a Risk Profile based on the sum of the frequency and severity of the occurrences. In one instance the airline Safety Manager was aware of this and his aspiration was to improve the system to take into account of the severity as well as the frequency; the case in point concerned the Despatcher falling from the aircraft steps – only one or two occurrences but the severity was high as the individuals received severe injuries.

It is considered that a hazard log should be supplemented by the standard FOQA system rather than the Risk Profiles replacing the hazard log.

2.2.7.1 Types of Hazard Log

There are a few companies providing bespoke hazard logs or tools for conducting and recording risk assessments. Although these are standard hazard log tools they may require tailoring to suit a specific project. Moreover, when undertaking hazard and risk management one should always be cognisant of what the outcome is to be i.e. what are you going to do with the identified and analysed hazard? Does it require linking to an accident? Is it a simplex accident sequence or must the relationships be able to cope with many-to-one and many-to-many linking and therefore be able to cope with different levels within the sequence? Is the tool able to represent both the Design Organisation information and also integrate this with the Operator Safety Risk Management?

Herein lays the issue with generic tools – they may be too simplistic or indeed not up to the task and hence do not get used. A hazard log should be based on user requirements. In this instance there is currently no detailed guidance for hazard logs except that of the minimum requirements detailed by the ICAO standards mentioned above. It is considered that due to the lack of an integrated safety

model the Design Organisations and Operators are left to their own devices and hence depending on the level of competence (or level of time and resource available) then the levels of hazard tracking vary enormously; this should be more consistent and more widely applicable – safety should not have standards within standards and organisations should learn lessons from one another in order to show continuous improvement.

Section 3.4 discusses a Hazard Log based on the Exemplar Safety Model.

2.2.8 Human Factors Integration

Human Factors are cited within accident board investigations as being contributory factors within an accident sequence.

Human Factors Integration (HFI) involves a multi-disciplinary team of experts that examine the requirements and issues concerning HFI during the early stages of aircraft/spacecraft development. It can also be termed Human Machine Integration (HMI) or Human Machine Ergonomics (HME)

Interfaces between humans and complex electronic elements should be analysed carefully such that human errors are minimised. Another factor to consider is that the 'machine' does not overload the human with information; particularly in fault scenarios i.e. multiple error messages as was the case on Air France Flight 447 (see 3.4.7 for the case study).

2.2.8.1 HFI Models

Useful models exist to examine these integration factors including the '*SHELL*' model and the 5-M model.

SHELL Model

The current *SHELL* model is based on Professor Edwards' model[13] which looked at the Software + Hardware + Environment + Live-ware (humans) aspects. It was not until 1975 that Captain Frank Hawkins added a second 'L' to the model to capture the interaction of the L-L i.e. humans with humans and in particular the management. Figure 21 below depicts the model.

Figure 21: SHELL Model adapted by Hawkins

5-M Model

Figure 22 below depicts the 5-M model[14] based on T P Wright and adapted by E A Jerome (1976) that best describes the interaction of **m**anagement, **m**an, **m**achine and **m**edia in order to either have a successful **m**ission or a **m**ishap. The following section describes known and emerging issues within

[13] http://www.skybrary.aero/index.php/ICAO_SHELL_Model
[14] http://en.wikipedia.org/wiki/5_M_factors

the aviation domain (the suborbital space domain issues are also described in this section for comparison).

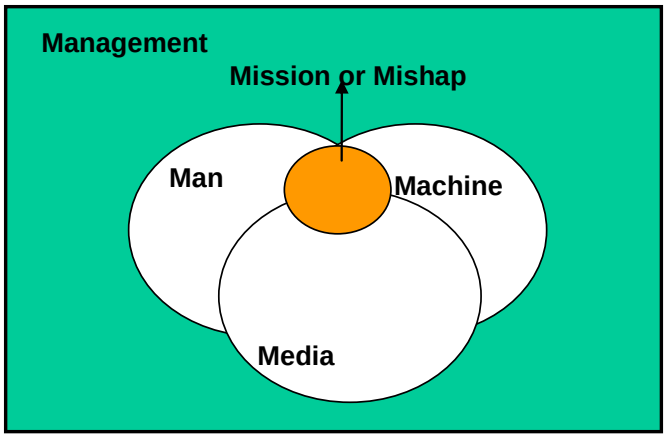


Figure 22: 5-M Human Factors Integration Considerations

Man

The Human Factor is the most variable element in the model and statistically is the greatest contributor to aircraft accidents (currently estimated at 90%[15]).

- Aviation/Current Space Issues;
  - Aviation;
    - The aviation industry has always suffered from 'cross-cockpit gradient' issues and this has led to accidents in some cases. Additionally where pilots are cited as being a major contributor in an accident, the root cause has sometimes not been uncovered; such as fatigue, lack of training, poor procedures. The Air France AF447 disaster is a prime example of this and this is covered in more detail in the case study at 3.4.7
  - Space;
    - Orbital spaceflight involves a large multi-disciplinary team and operator procedures are a key mitigating factor in preventing accidents. The accident review (summarised in Table 2) reveals that the mishaps were due to technical causes (machine) and management as opposed to direct human factor errors (man). That said there will be a lot of unreported incidents involving man on the Space Shuttle, Soyuz or indeed aboard the ISS and these are either unreported or reported within the closed system of NASA.
- Suborbital Issues
  - Flight Crew
    - Selection; Must be biased towards high-speed, high-g, high-stress previous experience (FAA state 'of similar experience').
    - Performance; Must have simulator training/test flights to improve performance and maintain standards.
    - Personal Factors; Crew Resource Management Training (CRM) to optimise synergy.

[15] http://en.wikipedia.org/wiki/Human_reliability

        - Flight Crew Fatigue; within the aviation domain there is growing concern regarding pilot fatigue as a contributor to human error in accidents and incidents. Within the suborbital domain although the flights are not long i.e. no more than one hour, fatigue must be considered in Operator's analysis. The rationale is that the flights may be more exacting on the pilots with the g-forces playing a major factor; it is anticipated that the pilots will experience up to +3g(z) during the pull-up phase and up to +6g(x) during the descent[16]. This may not be relevant during the test phase or early operational flights as the number of flights will invariably be low, however if flights are conducted more than once per day then fatigue will quickly become an issue.

          The UK CAP 719 [57] agrees with this cautionary point and state that 'acute fatigue is induced by long duty periods or by a string of particularly demanding tasks performed in the short term.'
    - Spaceflight Participants (SFP); this is not a joy ride and hence the suborbital flight will be exacting for the SFPs. Indeed some may not be able to withstand excessive g-forces and hence there is a need to consider the following:
        - Medical Screening; there must be an explicit list of 'go/no-go' conditions for SFPs
        - Training; centrifuge training is a key aspect and is not mandatory in the FAA-AST guidelines
        - Personal Factors. With comprehensive training and briefing, the passenger's psycho-physiological condition can be bolstered and SFPs should pose less of a risk to themselves and also such that they do not become a hazard to the control of the vehicle

Machine

The design of the aircraft/spacecraft is complex yet must meet certain certification requirements (or guidelines in terms of the FAA-AST for Suborbital design analysis within the United States)

- Aviation/Current Space Issues;
    - Aviation:
        - Only 10% of aviation accidents are cited as having design issues as the contributor i.e. towards a CFIT or LOC. Machines are becoming more complex and apart from composite design advancements, Complex Programmable Equipment (CPE) are perhaps providing more problems than the ones they were supposed to solve. In particular to the design and HFI issues, the Air France Flight 447 disaster cites misleading CPE as a contributor; this is examined in more depth as part of a case study in Section 3.4.7.
    - Space:
        - The Space Shuttle and Soyuz are complex systems requiring an extensive Rocket Propulsion System (RPS) in order to overcome the Earth's gravitational pull. Herein lays some of the problems with the machine and in particular to the Shuttle Challenger. Additionally the structural integrity of the machine must withstand immense forces during launch/ascent and re-entry in particular.
- Suborbital Issues

[16] Typical g-forces and flight time from the Virgin Galactic model; http://www.virgingalactic.com

- There are different design solutions currently in development and even test flights (Virgin Galactic). The vehicle designs vary in their launch and re-entry/approach methods including horizontal launch and take-off (XCOR), air-launch and glide to land (Virgin Galactic) and vertical take-off and land (Blue Origin). All of these are non-standard (aviation) designs using novel technologies and it is envisaged that these will present a high Safety Risk (at least one or two orders of magnitude 'less safe' than civil aviation standards). The novel design issues with Suborbital flight include:
  - Environment Control and Life Support System ECLSS
  - Rocket Propulsion System (RPS)
  - Propellant
  - Reaction Control System (RCS)
  - Composite Materials

Media

The environment can influence the aircraft/spacecraft

- Aviation/Current Space Issues;
  - Aviation:
    - Icing conditions (both on the ground and in flight – AF 447)
    - Wind-shear
    - Lightning
  - Space Issues
    - Space Debris
    - Solar Flares/general radiation
    - Re-entry temperatures
- Suborbital Issues
  - Extreme Altitude; high differential pressures, high temperature gradients
  - High 'g' forces
  - Radiation – negligible effect though worth considering
  - Space Debris – negligible effect though worth considering
  - Excessive Noise
  - Excessive Vibration

Management

The Management element has a large influencing effect on all of the elements and in particular to the man and the machine.

- Aviation/Current Space Issues;
  - Aviation;
    - The Air France flight AF447 disaster is a clear example of management being a major contributor to the accident (meaning Air France management not Airbus management – who did submit a Service Bulletin to change the pitot tubes); this is examined in more depth as part of a case study in Section 3.4.7.
  - Space;
    - NASA Management has been cited as major contributors to both Challenger and Columbia Space Shuttle disasters.
- Suborbital Issues
  - Regulation - Conforming to or exceeding regulations
  - Procedure - Control of crew procedures and ground control checklists, SOPs and Emergency procedures
  - Limitations – Suborbital flights need to have defined 'corridors' and be able to integrate with Air Traffic Management

- Flight Readiness Review (FRR) – the FRR will be a key management feature in the emerging Suborbital operations field. Safety Management of the Flight Crew, SFPs and the 'public' must be considered a top priority and this should be demonstrated by having the Safety Manager as a key stakeholder and with the authority to stop a flight. Additional stakeholders would include the Operation Officer (responsible for both operations and support [engineering/maintenance] and the Chief Medical Officer – all reporting to the Chief Executive; for this activity it is essential that a RACI chart is implemented whereby people know whether they are Responsible, Accountable, Consulted or Informed when a Go-No-Go decision is required (as well as the rest of their standard duties according to the RACI chart).

Mission

The mission element is the central focus of the model in that it summarises the operation. The mission is where the interaction of all the other elements combines to conclude in a mission success or a mishap. The mission is where the complexities of the operation are well defined, clearly understood and are attainable [29]:

- Aviation/Current Space Issues;
  - In aviation operations are routine and the flight planning aspect ensures that the mission is well defined. Possible issues here include other domains affecting the mission (media and man in particular) including last minute changes to the route or diversions due to external factors such as a runway blocked.
  - In orbital spaceflight the mission is a critical factor because of the exacting environment. The mission can be broken into the different phases because each phase has its own mission challenges in terms of interaction with the other elements and the main interactions are detailed below;
    - Launch; machine and management
    - Ascent; machine and media
    - Spaceflight; machine, man and media
    - Docking; machine, man and media
    - Re-entry, machine, media
    - Approach & Landing; machine, man and media
- Suborbital Issues;
  - As expected the suborbital mission is less demanding than the orbital mission but is more demanding than aviation operations and hence sits in the 'middle' sector in terms of challenges. As opposed to orbital vehicles the suborbital vehicles are different in design i.e. air-launched, aircraft-based ground take-off and land or vertical launch rockets. All of these have the same basic mission phases;
    - Launch (vertical, air drop, air rocket initiation [after normal take-off] or ground take-off); machine, man and media
    - Ascent; machine, man and media
    - Short Suborbital Space segment; machine, man and media
    - Approach & Landing; machine, man and media

    As can be seen the suborbital mission phases include 'man' within all phases as opposed to a lot of automation (machine) in the orbital phases.

HFI – Poor Examples

Examples of poor HFI include:

- Kegworth Air Crash; in this disaster the pilots shut down the wrong engine
  - Poor cockpit interface of multi-function displays
  - Inadequate warning system – engine fire detection (visual and audio)
  - Illogical spatial labelling – No's 1 & 2 engine (above and below and not left to right)
- Air France Flight 447 Crash; in this disaster the pilots failed to apply the correct actions when confronted with multiple failure warnings/cautions that were displayed on the Multi-Function Displays (the information is derived from the Air Data computer). This is examined in more detail in Section 3.4.7.

2.2.8.2 Human Error

The 5-M model above details the difficult issues that designers are faced with and it is clear that the human-in-the-loop is the most unpredictable part of the total system and the most difficult to model in terms of design and system safety analysis. Human error tends to be a failing in performance due to various influencing factors. These are best described from Reason's [58] analogy of Rasmussen's theory based on 'Skills-Rules-Knowledge' (SRK) performance levels in relation to errors:

- Skills-Based level; this is where we carry out a routine task in an automated way
- Rule-Based level; this is where there has been a situational change within the routine task and we need to change from a fully automated state to undertake a rule-based task based on procedures for example. In Figure 23 this is depicted in the 'mixed' state as we are 'trained for problems'; in some instances we will have to fully and consciously follow a procedure whereas other procedures may require practice so that the procedure is an automatic action such as in certain well-practised aircraft emergency procedures i.e. a double-engine failure on take-off (in a four-engine aircraft for example)
- Knowledge-Based level; this is where the situational change in a routine task is perhaps non-nominal and does not fit the 'rule-based' level such as an emergency with additional external factors. In this instance we have to rely on our knowledge to determine the actions to take.

These SRK performance levels take cognisance of both the human psychological state and situational variables from which Reason derived his SRK 'activity space' as depicted in Figure 23:

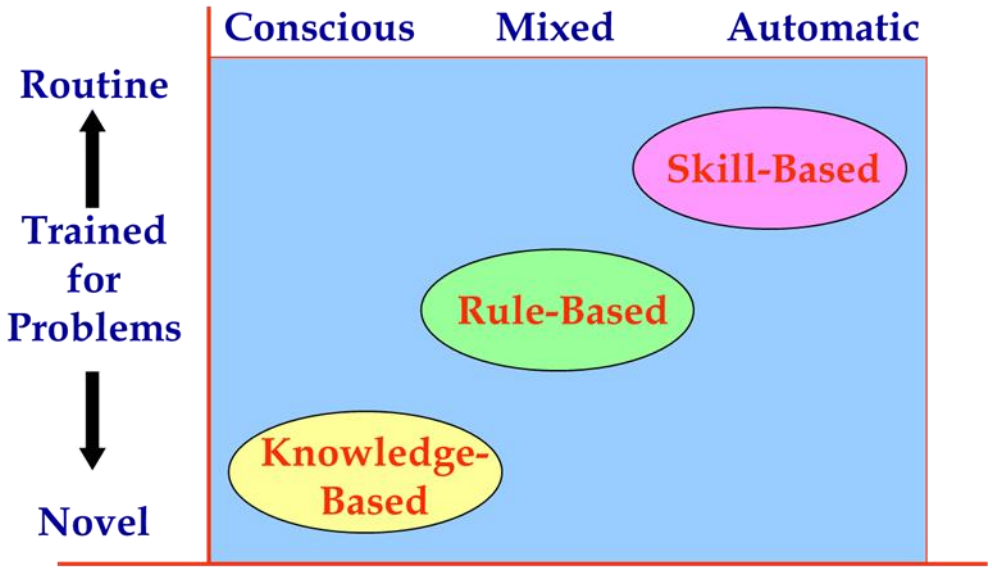


Figure 23: Reason's Skill-Rule-Knowledge based performance levels (based on Rasmussen) within the 'activity space'

Relating the SRK model to errors Reason then splits these into skill-based errors (slips and lapses) and mistakes (rule-based and knowledge-based mistakes). Additionally Reason suggests a third type of error and that is 'violations' whereby a deviation from a procedure occurs; here Reason suggests this can be deliberate or erroneous (though not for sabotage reasons). Reason also states that the SRK levels are not mutually exclusive and may coexist at the same time.

In another paper on Risk of Human Error by Chappelow [31] the analysis is refined and focuses on actual military accident and flying data combined with expert opinions in trying to quantify human performance aspects and in particular human error. Figure 24 below represents analysis of a mid-air collision accident in the form of an influence diagram generated by the experts.

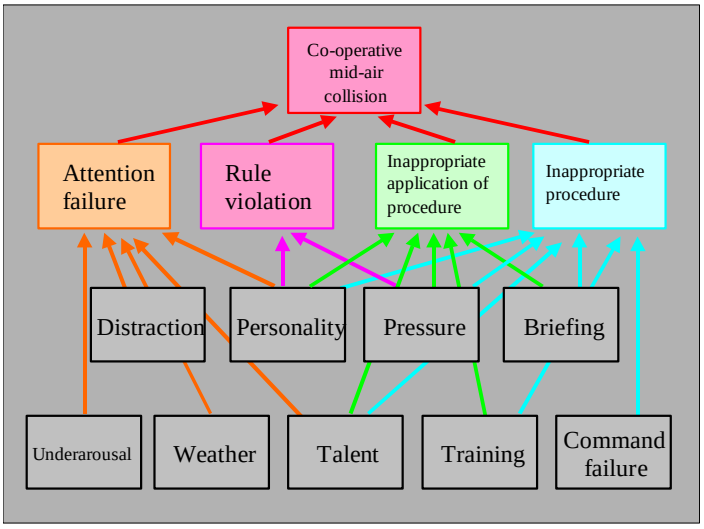


Figure 24: Chappelow's Influence Diagram on Human Performance and Errors

In relation to the SRK methodology we can see that the categories do coexist as Reason suggests. The following provides a consolidated and explicit list of Chappelow's detailed analysis with Reason's model (based on Rasmussen):

- Skills-Based error
  - Attention failure
    - Under-arousal
    - Distraction
  - Inappropriate application of procedure
    - Training (lack of or inexperience)
- Rule Based Error
  - Rule violation (deliberate or erroneous and not sabotage)
    - Personality
    - Pressure
  - Inappropriate application of procedure
    - Training (simple cognitive error)
  - Inappropriate procedure
    - Briefing (incorrect or lack of)

- Knowledge Based error
    - Inappropriate application of procedure
        - Personality
        - Talent
        - Training (cannot train for all eventualities in all environments)
        - Pressure

Human Error Probability

The above SRK can assist in further analysing the human error aspects in terms of applying probability values to human error in order to assist in modelling the total system (the author's view is that this is aimed at the operator's safety risk management in terms of procedures and training – as opposed to designers using HMI analysis separately to design out human interface issues therefore the designer's aim is still to meet the safety objective by safe design practices i.e. not taking credit for human error probability within the analysis).

A Human Interface Error Probability paper [30] provided common human error probability data from Kirwan as depicted in Table 8 below:

Description	Error Probability
General rate for errors involving high stress levels	0.3
Operator fails to act correctly in the first 30 minutes of an emergency situation	0.1
Operator fails to act correctly after the first few hours in a high stress situation	0.03
Error in a routine operation where care is required	0.01
Error in simple routine operation	0.001
Selection of the wrong switch (dissimilar in shape)	0.001
Human-performance limit: single operator	0.0001
Human-performance limit: team of operators performing a well-designed task	0.00001

General Human-Error Probability Data in Various Operating Conditions

Table 8: Human Error Probability Data from B Kirwan

Another source of human error probability data is from Def-Stan 00-56 [32] and is more focused on defence systems and specifically applied in aircraft-based human errors. Here the term 'omission' error relates to skipping a part of a task and 'commission' errors relate to incorrectly performing a task:

Nature of task	Failure probability
General omission error, when there is no warning alarm or display	10^{-2}
Errors of omission when the actions are embedded in a well-rehearsed procedure	3×10^{-3}
General error of commission	3×10^{-3}
Simple arithmetic errors with self checking	3×10^{-2}
General error of supervision	10^{-1}
Handover/changeover error	10^{-1}
General decision error rate for high stress levels	0.2-0.3
Failure to act correctly in reasonable time after the onset of a high stress condition, e.g. a loss of coolant accident in a nuclear reactor	0.3-1.0

Table 9: Human Error Probability values applied for aircrew in military analysis

In comparison the two approaches are similar and we can therefore apply the probabilities for the SRK methodology as follows:

- Skill-Based errors
  - Error in simple routine operation = 0.001 ($1x10^{-3}$)
  - General error of commission = 3×10^{-3}
- Rule-Based errors
  - Errors of omission when the actions are embedded in a well-rehearsed procedure = 3×10^{-3}
  - Error in a routine operation where care is required = 0.01 ($1x10^{-2}$)
- Knowledge-Based errors
  - Operator fails to act correctly in the first 30 minutes of an emergency situation = 0.1($1x10^{-1}$)
  - General omission error where there is no warning alarm or display = $1x10^{-2}$
  - General rate for errors involving high stress levels = 0.3 ($3x10^{-1}$)
  - General decision errors rate for high stress levels = 0.3 ($3x10^{-1}$)

These performance levels can coexist and herein lays the issue in terms of accurately modelling the probability values. For simplicity the following guide (based on the above comparisons) could be applied to aircraft/spacecraft operational safety risk management and this is discussed further in 3.4.6.3:

- Control measures for high Stress emergency situations = 2×10^{-1}
- Control measures for well-rehearsed procedures to prevent a hazardous situation = 5×10^{-2}
- Control measures for simple routine operations = 3×10^{-3}

Training is a difficult factor to quantify and the following is considered reasonable to take credit for within a safety analysis:

- Training for normal (green) procedures = 0 i.e. no additional credit
- Training for abnormal (amber) procedures = 5×10^{-2}
- Emergency Training (red) = 2×10^{-1} per flying hour based on the high stress situations

Implementing a Limitation is also a difficult factor to quantify because if a Limitation is in place and is followed to the letter then the hazardous situation (or accident) should not arise. However as with

all human-based actions there are situations that flight crew may go against the limitation; this could be as a Rule-Based Error or an unforced situation arises whereby the pilot uses his judgment during an emergency drill for instance i.e. a Knowledge-Based Error:

- Limitation = 1×10^{-2} per flying hour based on the general omission error where care is required or general error of supervision

All of the above derived values are proposed for the safety model, however it is important that the relevant stakeholders (in particular flight crew, the safety manager and systems analyst) are consulted and agree upon the relevant values that can be credited within the accident sequence and therefore Risk Estimation.

2.2.9 Safety Culture

The above section on Human Factors discussed the 5-M model whereby the **m**anagement have a large influencing factor on the safety of the mission (and its success or not). Additionally the section also discussed human errors (the **m**an part of the model) and some of the reasons for variability in human performance. These issues can only be counteracted by the implementation of a top-down, bottom-up safety culture.

The ICAO SMS Manual [24] discusses safety culture in terms of the 'just culture' defined in Professor James Reason's book on Organizational Accidents [58]:

> *"The attempts to protect safety information and the reporter from punishment were developed using the term culture, for example, "non-punishing culture", "non-blame/blame-free culture" and lately "safety culture" or "just culture". The word culture does have specific meanings and the context in which it is used in this case can lead to misperception and misunderstanding. Nevertheless, safety and just culture have become broadly accepted, although not universally defined, terms to describe the context in which safety practices are fostered within an organization."*

The UK CAA discusses safety culture in terms of commitment from the safety policy:

> *"In preparing a safety policy, Senior Management should consult with key staff members in charge of safety-critical areas. Consultation will ensure that the safety policy and stated objectives are relevant to all staff and that there is a sense of shared responsibility for the safety culture in the organisation. A positive safety culture is one where all staff must be responsible for, and consider the impact of, safety on everything they do."*

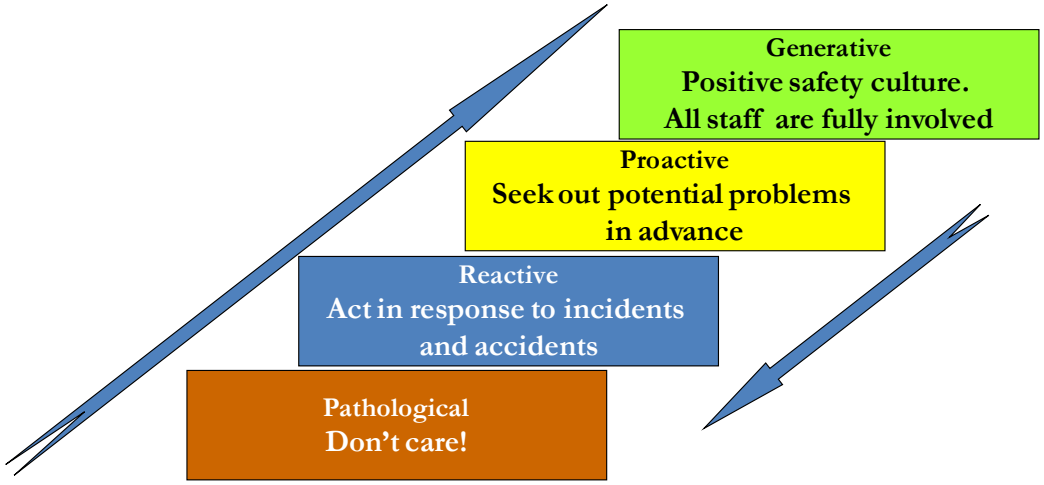


Figure 25: Professor James Reason's Safety Culture Model

In terms of safe operations there is no denying that whether in the commercial side of aviation or in the military everyone is trying hard in terms of 'flight safety' and evidence of this will no doubt be in the forefront of their statistics (aircraft loss rate). Flight Safety tends to be more of a reactive disposition and this is shown quite aptly in Professor James Reason's diagram in Figure 25 above. As can be seen from the 'reactive' culture, an organisation has some way to go towards becoming a 'generative' culture. In today's climate of scant resources due to cut-backs in most departments it is difficult to try and introduce new measures to improve an organisation's safety culture. Indeed and in particular to the military, entrenched cultures are sometimes difficult to shake-off. Nonetheless every Safety Manager must attempt demonstrate 'Continuous Improvement' as demanded of overarching safety governance such as the ICAO SMS or from the equivalent governance within the military.

Breaking the chain within an accident sequence is more likely to happen with a proactive or generative safety culture. Figure 26 shows how maintenance (the **m**an in the 5-M model) could break the chain with pre-flight inspections or undertaking a task effectively as part of a maintenance schedule. In the Challenger disaster it was the management that could have broken the chain by not launching at such a cold temperature and in the Air France AF447 disaster the management could have introduced limitations and the pilots could have broken the accident chain by avoiding the icing conditions or taking the correct actions (procedure) in the hazardous situation.

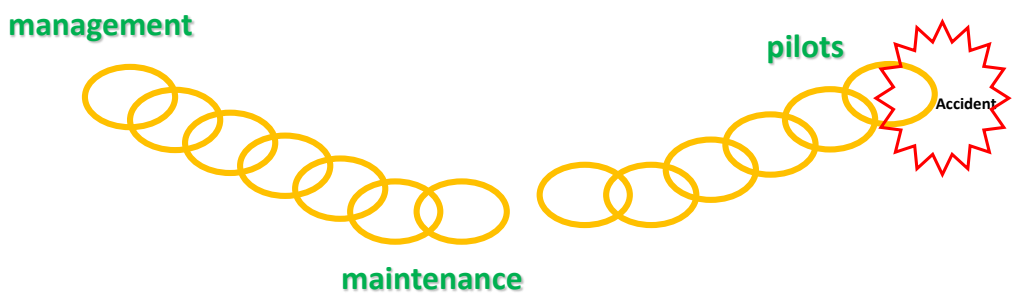


Figure 26: Breaking the chain in an accident sequence

In terms of the emerging suborbital space industry the fore-runners such as Virgin Galactic, XCOR and Armadillo Aerospace these companies should be proactively encouraging and implementing a safety culture; this is discussed in 2.3.13.

2.2.10 Commercial Operations

This section provides an overview of the safety management activities concerning the commercial operators. The review focuses on the requirements and guidelines presented to operators in order to manage the safety effort for their airline.

2.2.11 EU-OPS

EU-OPS 1.037 [59] stipulates that Operators must have a 'Flight Safety' programme to be able to obtain an Air Operator Certificate. The document also covers those requirements such as safety and emergency equipment and safety training. In terms of 'OPS 1.037', an operator must establish:

Accident prevention and flight safety programme:

> *(a) An operator shall establish and maintain an accident prevention and flight safety programme, which may be integrated with the quality system, including:*
>
> 1. *Programs to achieve and maintain risk awareness by all persons involved in operations; and*
> 2. *An occurrence reporting scheme to enable the collation and assessment of relevant incident and accident reports in order to identify adverse trends or to address deficiencies in the interests of flight safety. The scheme shall protect the identity of the reporter and include the possibility that reports may be submitted anonymously; and*
> 3. *Evaluation of relevant information relating to accidents and incidents and the promulgation of related information, but not the attribution of blame; and*
> 4. *A flight data monitoring program for those aeroplanes in excess of 27 000 kg. Flight data monitoring (FDM) is the pro-active use of digital flight data from routine operations to improve aviation safety. The flight data monitoring programme shall be non-punitive and contain adequate safeguards to protect the source(s) of the data; and*
> 5. *The appointment of a person accountable for managing the programme.*

The flight safety program will typically include a Risk Assessment scheme based on the ICAO SMS and also employ 'Risk Profiles' as detailed in 2.2.7.

2.2.12 ARP 5150

ARP 5150 [75] concerns the safety assessment of transport airplanes in commercial service and has useful guidelines, tools and methodologies for airline safety managers to follow. The document's stated intent is that operators should:

- *Maintain the airworthiness (certification) of the airplane – in service events are assessed based on the effects of the level of safety intended in the certification process*
- *Maintain the safety of the airplane – in service events are assessed against the internal safety objectives of (the) your company*
- *Improve the safety of the airplane – in service events are assessed to identify opportunities to decrease their number, or to surpass the safety objectives of (the) your company*

These statements are important and indicative of the theoretical approach to managing operator safety risks; indeed steps 'b' and 'c' are clearly achievable depending on what 'internal safety objectives' are set by the operator's safety manager i.e. no more than 2 deaths per year or no more than 10 Safety Significant Events per month and so on. The term 'safety objective' should not have been used here and it clearly demonstrates the lack of joined up approach that exists in the aerospace business today. Instead, the term 'safety goal' would have been preferable and therefore it would not be confused with the term associated with a failure condition i.e. a catastrophic failure condition's safety objective (for Part 25 aircraft) is $1x10^{-9}$ per flying hour. The second and third goals (maintaining and improving the safety of the airplane) are effective and quite achievable.

However the interesting statement is that of the first statement above – to maintain the airworthiness of the aircraft (based on the effects of **the level of safety** intended in the certification process). This stated intent is most important yet appears to stop there; both in the document and at the airlines[17]. There is no contiguous assessment of the level of safety achieved at certification to that of the Risk Profile scheme or individual Risk Assessments undertaken by the operator (indeed the two visited did not have hazard logs but preferred the Risk Profile scheme as part of the FOQA). Hence it is the author's view that airlines are still undertaking 'Flight Safety' activities (more reactive approach) rather than employing a fully integrated Safety Management System (proactive approach).

2.2.13 FAA SMS for Operators

The FAA has provided AC120-92 [33] which is an introduction to SMS for operators. The guide is designed to '*allow integration of safety efforts into the operator's business model and to integrate other systems such as quality, occupational safety, and environmental control systems that operators might already have in place or might be considering'*. The guide is well presented and follows ICAO's '*Four Pillars of Safety Management'* (2.2.2) with the overall safety risk management and safety assurance process depicted in Figure 27 below. Their approach is sound and they adopt a '*systems of systems'* approach whereby they recognise that a 'system' can be *equipment, people and facilities*. Therefore they are adopting a systems safety approach by analysing the risks involved at the 'system' level whereby they recommend that *the most effective method of risk reduction is by brainstorming with company pilots, mechanics or dispatchers* for instance.

The guide has reasonable safety criteria with severity and likelihood classifications that have been adapted from the ICAO SM Manual and a standard safety risk matrix; the safety risk matrix is simplistic with an acceptable, acceptable with mitigation and unacceptable risk region.

[17] Based on the author's view of visiting two major airlines

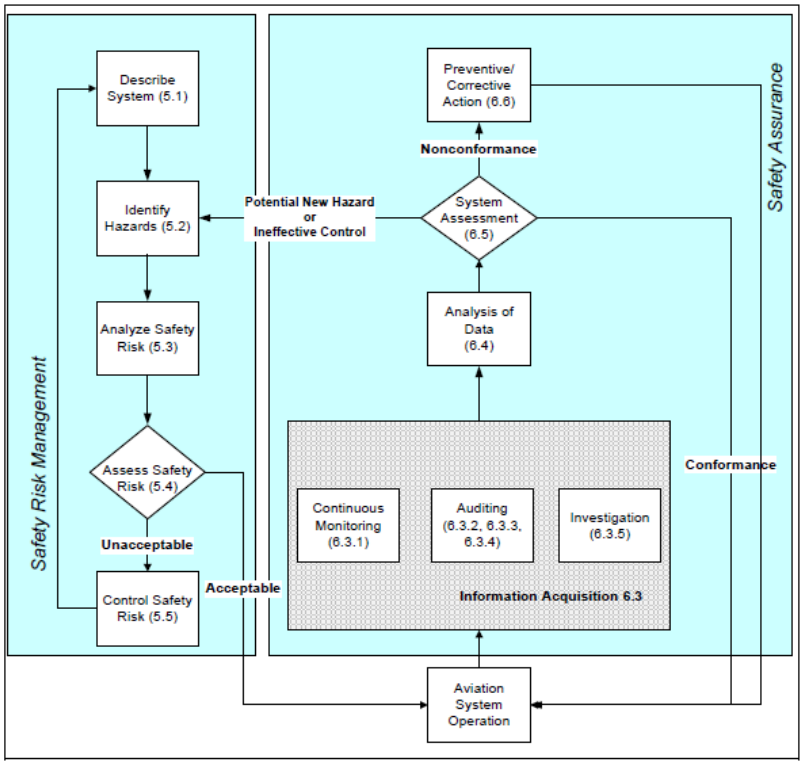
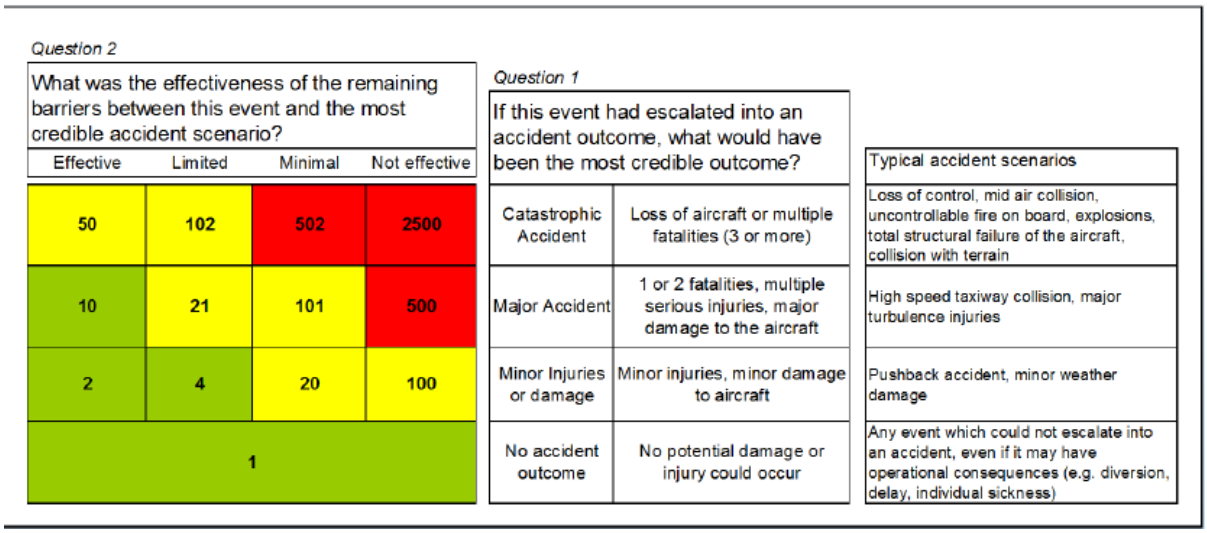


Figure 27 : FAA Operator's SMS Methodology

2.2.14 Aviation Risk Management Solution

The Aviation Risk Management Solution (ARMS) methodology [34] is a reasonable attempt at providing a system for operators to assess their risks by introducing an Operational Risk Assessment (ORA) process. The ARMS methodology and Excel spread-sheet (tool) is aimed at airlines and other air operators and is based on a two-tiered approach including a preliminary Event Risk Classification scheme followed by a more specific Safety Issues Risks Assessment (SIRA).

The rationale stated in the methodology is that '*pre-ARMS' standard methodology is not anchored to any recognised industry reference'* (in terms of Operator Risk Management Matrices with severity and probability); this is correct and hence this thesis has also recognised this but has focused on a new safety model that provides a contiguous safety approach i.e. the operator analysis **is** anchored to the design analysis and the metrics (per flying hour) are constant (see Chapter 3.4). Additionally the method contained within the SIRA provides a weighting for the failed 'barriers' (which is a good approach) however it is based on an estimated failure rate **per sector** as an example i.e. there is no relation or reference to human error rates. There are two problems with this approach: the first is the use of sectors as this does not correlate to flight hours; the second is that the estimations may not be conservative enough (as they do not relate to human error analysis) and therefore the resultant 'risk' may be biased towards a lower value hence hiding the real risk. Within the Event Risk Classification matrix the metrics have been derived from accident data and appear irrelevant and based on aircraft loss values. Nonetheless the usefulness of the matrix is that it is a starting point that identifies high and medium risks that require further analysis i.e. in the form of a SIRA.



Question 2

What was the effectiveness of the remaining barriers between this event and the most credible accident scenario?

Effective	Limited	Minimal	Not effective
50	102	502	2500
10	21	101	500
2	4	20	100
1			

Question 1

If this event had escalated into an accident outcome, what would have been the most credible outcome?

		Typical accident scenarios
Catastrophic Accident	Loss of aircraft or multiple fatalities (3 or more)	Loss of control, mid air collision, uncontrollable fire on board, explosions, total structural failure of the aircraft, collision with terrain
Major Accident	1 or 2 fatalities, multiple serious injuries, major damage to the aircraft	High speed taxiway collision, major turbulence injuries
Minor Injuries or damage	Minor injuries, minor damage to aircraft	Pushback accident, minor weather damage
No accident outcome	No potential damage or injury could occur	Any event which could not escalate into an accident, even if it may have operational consequences (e.g. diversion, delay, individual sickness)

Figure 28: ARMS' Event Risk Classification matrix

Issues with the ARMS methodology include:

- No human factors reference in terms of 'barriers' failing – they estimate the probability for a barrier failing 'per sector' i.e. 1 in 100 and 1 in 10,000 and so on; these are for 'avoidance barriers' (before the undesirable operational state) and 'recovery barriers'.
- Based per sector i.e. '*estimated frequency of triggering event*' is per flight sectors i.e. every 100,000 ($1x10^{-5}$). The issue here is that the estimations can be optimistic or pessimistic depending on the safety analyst. Additionally the tool allows for a single sector analysis to determine whether the route may be acceptable; this would seem like a good idea however this results in an unacceptable risk due to the frequency of '1' being inserted in the tool. Their answer to this is that '*with the excuse that exposure to those elements within the global operation is very limited'*
- The system can be tailored to the 'customer' and it is stated that the same ERC can be used for different applications such as;
    - *Risk per airport*
    - *Risk per flight phase*
    - *Risk per time of year*

  This is also commendable but is it practical to attempt to cover the risks of 'x' per 'y' for different metrics within the same risk classification system? Arguably the risk at airports would be risk of death per person per year (per group or event i.e. despatchers, maintainers, flight servicing, air traffic controllers, etc.) whereas the risk for aircraft concerns the sectors (as detailed above)
- Also tries to address safety issues on a global risk map meaning that they are attempting to have a common approach across airlines and other operators; this is commendable but not practical

The ARMS methodology intent is useful and has chosen the metric as 'per sector' because there is indeed no anchor to any prevailing metric in use today (design organisation or otherwise). However this relies a lot on estimation and may not be updated sufficiently to maintain a robust model. The use of an 'undesirable operating state' is also useful and is based on the 'BOW-TIE' approach with avoidance barriers and recovery barriers as depicted in the SIRA framework model at Figure 29 below. Here the methodology attempts to provide a weighting for risk reduction (controls) and once

again this is based on 'conservative estimation'; without reference to human error probabilities these estimation can easily be manipulated to achieve a positive outcome.

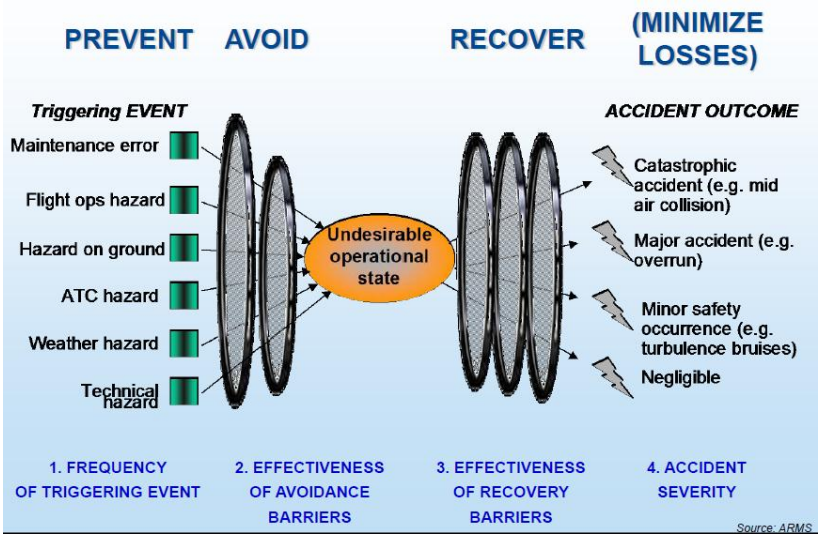


Figure 29: ARMS' Safety Issues Risk Assessment Framework

2.2.15 GAIN Operator's Flight Safety Handbook

The Global Aviation Information Network (GAIN) Working Group have developed an Operator's Flight Safety Handbook [35] in order to *serve as a guide for the creation and operation of a flight safety function within an operator's organisation*. The handbook covers the following topics:

- *Organisation and Administration*
- *Safety Program Activities*
- *Human Factors*
- *Accident/Incident Investigation & Reports*
- *Emergency Response & Crisis Management*
- *Risk Management*
- *Organisational Extension*
- *Cabin Safety*

The Appendices provide additional methods, tools and processes and in particular Appendix E 'Risk Management Process' provides a useful insight into the Hazard Identification process; not only from the operator's perspective but discusses system complexities, system risks and system-based accidents. The section (E3.6.6) then provides a number of examples showing an accident sequence along with their *initiating hazards, contributory hazards and primary hazards* and *appropriate controls*. The point of the examples is to illustrate the accident sequences and to show the 'different' sorts of hazards previously mentioned. Figure 30 below shows one of the examples. Arguably the sequence is too simplistic but the points are well made; indeed the term 'primary hazard' is interesting and is not far from the author's introduction of a 'Key (Platform) Hazard (see Chapter 3.4.4).The guidebook's Appendix E also contains an example *Risk Analysis Matrix* with the simple severity of 0-5 and the following consequences:

- *People*
- *On time departures*
- *Assets*
- *Environment*
- *Reputation*

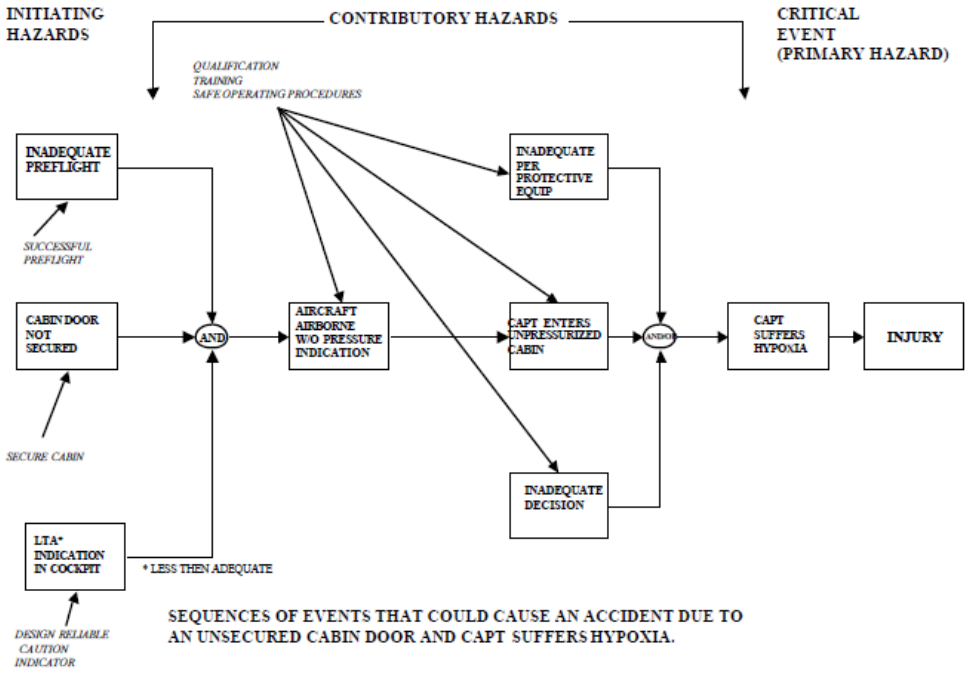


Figure 30: GAIN's Operator's Flight Safety Handbook Accident Sequence

2.2.16 Validation & Verification

This section reviews current validation & verification (V&V) methods and their relevance in the safety lifecycle.

2.2.16.1 Safety Validation

ARP 4754 [39] defines validation as:

> *Validation of requirements and specific assumptions is the process of ensuring that the specified requirements are sufficiently correct and complete so that the product will meet applicable airworthiness requirements.*

Validation is a key part of the design process in that the aim is to provide assurance that the product is viable to move on to the next phase of the development program; hence it is an iterative process during the early stages as shown in the system safety process diagram in Figure 31 and also on the left of the V-diagram in Figure 32.

The hierarchical requirements are defined at aircraft level, system and sub-system levels. In terms of safety the top level aircraft FHA is used in the first instance to establish Safety Requirements. Additionally safety requirements can be established from the aircraft level User Requirements and Regulatory Requirements including safety targets and objectives. Additionally it is important to establish assumptions at the beginning of a program and these should be validated to ensure that they are *explicitly stated, disseminated and justified by supporting data.*

Requirements are flowed down to system and sub-system level and therefore they cross boundaries (of function and responsibility). In terms of safety requirements it is important that these boundaries are clear and that they are explicitly detailed within a Validation Requirements Matrix; for instance a system may be apportioned a 'risk budget' of the overall safety target and then a sub-system may be apportioned a further portion of the 'risk budget' as a failure condition's safety objective. This is the

same for descriptive safety-related requirements. The validation at the initial aircraft FHA level is essentially validation of the safety requirements as depicted in the blue circle in Figure 31 below.

Additionally as the design develops further requirements are derived which may not have been related to a higher-level requirement; these are then termed derived requirements and in terms of safety analysis are therefore called derived safety requirements. These may also be 'flowed-down' to sub-systems.

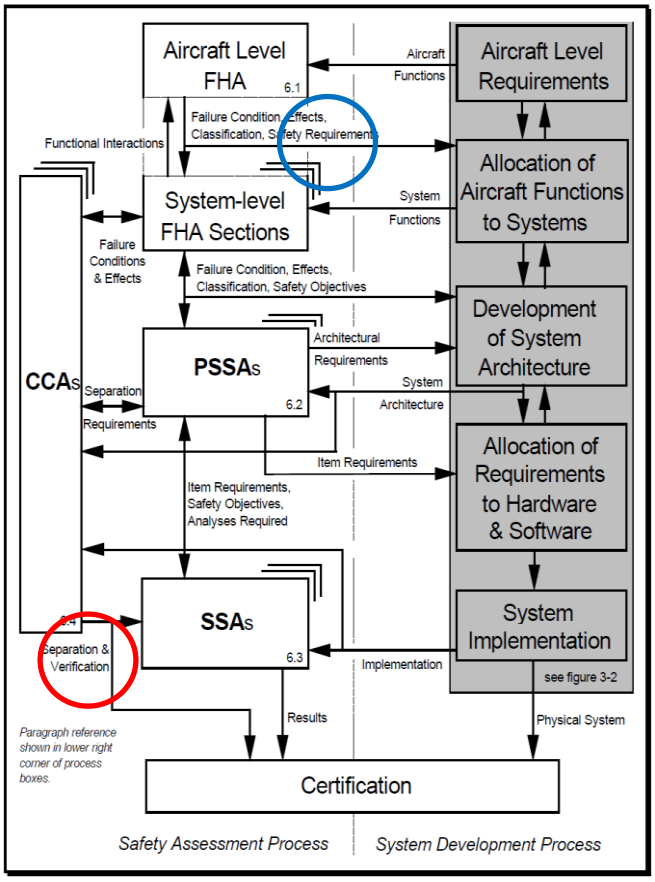


Figure 31: System Safety Process detailing Validation (blue circle) and Verification (red circle)

In terms of the requirements being *correct* and *complete*, ARP 4754 provides useful guidelines to address safety validation aspects:

- *Do requirements trace to identified sources*
  - *Intended functions – aircraft level, system level*
  - *All functions, hazards and failure condition classifications identified in FHA*
  - *All failure conditions incorporated in PSSA*
  - *Derived requirements – design decision assumptions*
  - *Applicable regulatory standards and guidelines*
  - *Anticipated operating environment*
  - *Established flight operations/ maintenance procedures*
- *Are Assumptions correct*
  - *FHA failure condition classification assumptions confirmed*
- *Do requirements correctly reflect the safety analysis*
  - *Appropriate safety analyses completed correctly*
  - *All system hazards identified and classified correctly*
  - *Impact of unsafe design or design errors*

- *Reliability, availability and fault tolerance requirements*

A validation plan is required to map out the validation process which consists of (from ARP 4754):

- *The methods to be used*
- *The data to be gathered or generated*
- *What should be recorded (such as: summaries, reviews, or investigations)*
- *The means for timely access to requirements validation information*
- *How the status of validation will be maintained, or managed, when changes are made to requirements*
- *Roles and responsibilities associated with the validation*
- *A schedule of key validation activities*

This validation part of the safety process is clearly vital and therefore the safety manager should ensure that this is effort is included in the safety program and is sufficiently resourced. If this is not completed correctly or even undertaken by safety personnel then the verification aspects will be extremely difficult to justify and the robustness of the 'as designed' safety case will be affected.

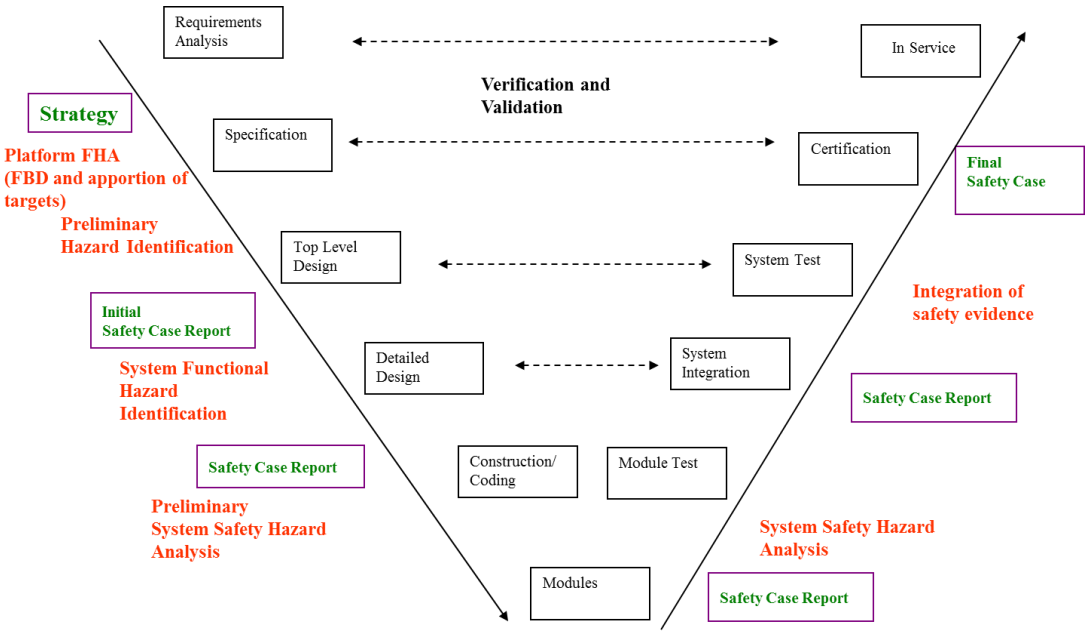


Figure 32: Design 'V' model detailing Validation & Verification activities with associated safety analysis

2.2.16.2 Safety Verification

ARP 4754 [39] defines verification as:

> *The evaluation of an implementation of requirements to determine that they have been met*

Verification ensures that the validated requirements have been satisfied and that the safety analysis remains valid. In terms of the system safety process this is later in the program as depicted by the red circle in Figure 31 above. ARP 4754 suggests that there are four basic methods of verification:

- *Inspection and Review*
- *Analysis*
- *Test*
- *Service Experience*

As with the validation process it is essential to have a plan for the verification activities; in particular detailing the roles and responsibilities of the stakeholders and detailing the level of independence required. The evidence gained from the various verification methods will enable a Verification Matrix to be completed which will form the basis of a verification summary for the design (System or Sub-system).

The Systems Hazard *Analysis* (SHA) is one method used for verification (ARP 4761 uses the terms System Safety Analysis (SSA) [39]) as depicted in the right side of the 'Vee' of Figure 32 above. ARP 4761 details the purpose of an SSA as:

(a) Verification that the design requirements established in the System Level FHA are met

- *Validation that the classification established for the aircraft level effects are justified*
- *Verification that the safety requirements called out in, or derived from aircraft design requirements and objectives are met*
- *Verification that the design requirements identified in the CCA process are met*
- *Linkage of the System level SSA to the aircraft level FHA.*

2.2.16.3 Other Industry & Academia Views on V&V

In a paper on design verification and analysis for the CIRP Annals, it is suggested "*that current validation and verification-based approaches mainly focus on product conformance to specifications, product functionality and process capability and that the current process can be subject to failures*." The paper provides concepts of validation and verification in the product lifecycle by including analysis and review of literature and state-of-the-art in:

(i) preliminary design,
(ii) digital product and process development;
(iii) physical product and process realisation;
(iv) System and network design; and
(v) complex product verification and validation.

The paper touches on the *future trend in requirements for early design verification* and suggests that there will be "*challenges in methods to deal with verification using low design data-intensity, to enhance the scope of functional verification with the development of integrated functional mock-up and techniques for the integrated product and process verification*."

With emerging and complex technology it will indeed be challenging and some of these aspects are reviewed more closely in the suborbital space safety section 2.3 and 2.3.14 concerning V&V.

2.2.17 Safety Independence

This section of 'safety tools review' has purposely been left to the last because once the 'safety case' is complete (for a particular milestone in the development program) and prior to its submission it should have the endorsement of an Independent Safety Auditor (ISA) as part of providing safety 'assurance' of the aircraft/spacecraft.

The author has been involved with many programs with and without an ISA and in some cases there has been confusion as to which organisation is doing what in terms of independent assurance of the 'product'. Within the UK MoD the author has come across the following terminology:

- Independent Safety Auditor – this is the correct role for the term 'ISA' and

involves an independent check to determine whether the System is compliant to safety requirements and targets/objectives. Indeed this role of the ISA is the only one considered in Def-Stan 00-56 [28];

An individual or team, from an independent organisation, that undertakes audits and other assessment activities to provide assurance that safety activities comply with planned arrangements, are implemented effectively and are suitable to achieve objectives; and whether related outputs are correct, valid and fit for purpose.

- Independent Safety Advisor – this is the role of a safety specialist (or team of specialists) whom support the Project Team in its safety activities.
- Independent Safety Assessor – this is the role of specialist technical personnel who are Subject Matter Experts (SMEs) in particular systems i.e. hydraulic specialists and who are capable of providing an independent assessment of a particular system as to its safe use.

Haddon-Cave [9] also believed this and cites 'there is an inconsistent approach to this separation of assurance and 'ensurance' and that this is further muddied by an unclear separation between advice and assurance in some areas' and that 'These differences are manifested in different degrees of independence and also various interpretations of the "A" as meaning advisors, assessors, assurers, auditors and also in different degrees of mandating of an ISA.

Indeed as a result of Haddon Cave's report the third group 'Assessor' have since become known as Independent Technical Evaluation (ITE) i.e. this is the role QinetiQ played in the Nimrod safety effort and indeed continue to do so on many MoD aircraft because of their expertise – in particular their facilities at Boscombe Down.

The role of an ISA (auditor) to provide Assurance is extremely important and an ISA should be engaged at the beginning of a project and then used at the various important meetings and in reviewing important safety documents. The rationale of having an ISA at the beginning of the project (rather than at the end just to check for compliance) is that a project should explicitly know its safety requirements and targets/objectives and these should be agreed at the beginning. A Functional Block Diagram and high-level Functional Hazard Analysis should be undertaken in the first instance to apportion safety objectives and to determine whether a project should actually progress. It is here at the beginning where an ISA can prove his worth in assuring that the project is actually viable (in terms of achieving the safety target and objectives).

2.2.18 Conclusions of Safety Tools Review

The 'Safety Tools' review provided a view that there are similar safety management methodologies employed in different organisations and also at different levels i.e. at the top, the ICAO SMS provides the top-level guidance and then within regulatory bodies (the FAA, EASA) further guidance is available. It is concluded that the majority of safety management tools and methodologies are similar, however particular definitions are different and where this was the case the author provided an exemplar definition to carry forward to Chapter 3. Examples of this included:

- Accident 'v' Mishap
- Safety Management System
- Cause 'v' Causal Factor
- Sectors 'v' Flying Hours
- Hazards 'v' Failure Conditions

The review highlighted good 'best practice' advice for Systems Design Analysts and provided clear safety objectives for the aircraft's failure conditions. Additionally the standard system safety engineering is considered best practice and there are suitable recommended guidelines such as ARP 4761 and ARP 4754. These, along with the higher-authority guidelines, provide the roadmap to effective safety engineering and safety management approaches; these start with the Safety Management Plan (and designer-based System Safety Program Plan) which contain the safety requirements and plans for hazard management starting with the Functional Block Diagram and FHA through to the verification stages including the System Hazard Analysis. However it must be noted that Design Organisations are interested in obtaining airworthiness certification for their aircraft and their liability seems to stop there (in terms of managing any operating risks); apart from distributing Service Bulletins for corrective action there is no intent to bridge the gap into the operator domain.

The system design effort follows the standard 'V' lifecycle whereby Validation and Verification (V&V) forms an important part of the process. The safety V&V effort follows the design lifecycle and reports on the status of meeting safety requirements and targets at each milestone; this is essential in determining whether the design is acceptably safe in moving to the next stage.

Today's aircraft designs employ software and complex hardware and these must be managed both in terms of compliance (of product assurance and process assurance) and also that the functional flow paths have been traced up to the sub-system and system level hazards. In a project that the author was involved in it was evident that the CPE certification personnel were only concentrating on the process and product assurance and left the safety aspects to the safety team (who believed that it was the CPE experts responsibility to deal with and merely required a summary from them); hence the author identified this serious gap in the safety effort - which was then at the test evaluation phase.

The review also highlighted that Operator-based Safety Management guidance was available however based on the author's limited visits to airline operators it appears this is not being put to good use; instead airline's Safety Managers tend to follow the FOQA approach and undertake Risk Assessments on an Incident-by-incident basis and use a Risk Profiling scheme. It was noted that ARP 5150 provided a number of safety management techniques that airlines could follow however these were still bespoke and operator-focused. Also the ARMS technique provided a reasonable attempt to provide guidance for operator safety risk management but once again this methodology is used in isolation and based on sectors as opposed to flight hours and uses bespoke metrics. To obtain an Air Operator Certificate (AOC) the airline must show that they have followed the safety management guidelines and as part of the AOC operators must implement a Safety Management System per ICAO guidelines.

It is concluded that the extant guidelines do not provide a methodology or approach that considers through-life safety management i.e. a contiguous safety model; rather there is separate guidance for system safety engineering (for DOs) and separate guidance for Operator Safety Risk Management. These shortcomings will be addressed in Chapter 3 by attempting to bridge the identified gap by a new safety model and this will be validated by the use of case studies.

2.3. PERSONAL SPACEFLIGHT INDUSTRY REVIEW

This section of the review concerns examining the foundations of the emerging Industry and undertaking an analysis to determine whether the 'Rules' and 'Guidance' are robust. As the Industry is in the developmental stage and gearing up for the Test & Evaluation phase, it was determined that a Gap Analysis would be beneficial (see 1.5.3); this Chapter establishes the 'current position' and Chapter 3 proposes methodologies towards a 'future state'. The rationale is that rather than just being told what is considered not robust or indeed incorrect, the Operators and European Regulators could be shown a more robust strategy to be able to take forward and adapt to their own requirements.

2.3.1 FAA Legislation, Regulations & Guidelines

Currently the FAA is leading the way in providing governance to allow Personal Spaceflight to take wings. The AST have provided the following Rules and Guidance for the prospective spacecraft designers and operators and the following sections will review the relevant safety aspects:

- *Legislation (Commercial Space Launch Activities)*
- *Regulation*
  - *General*
  - *Procedures (on regulation, licensing and Investigation Requirements)*
  - *Licensing*
    - *Parts 414 – Safety Approval*
    - *Parts 417 – Launch Safety*
    - *Parts 431 – Launch & Re-Entry of Re-Launch Vehicles (RLV)*
    - *Parts 460 – Human Spaceflight Requirements*
- *Advisory Circulars*
  - *Hazard Analysis for Re-Launch Vehicles (RLV)*
  - *License application procedures*
  - *Insurance conditions*
  - *Expected Casualty Calculations for Commercial Space Launch & Re-entry Missions*
  - *Reusable Launch & RLV system safety process*
- *Guidelines*
  - *Financial Responsibility Requirements*
  - *Failure Probability Analysis*
  - *Environmental guidelines*
  - *Safety Approval Guidelines*
  - *RLV Guidelines*
    - *Software Safety*
    - *Safety Critical Structure Analysis*
    - *Safety Critical Hardware Analysis*
    - *RLV Safety process*
    - *Safety Validation and Verification Analysis*
    - *RLV Operations & Maintenance*
    - *Medical Screening guide*
    - *Operations with Flight Crew Guide*
    - *Operations with Spaceflight Participants guide*
    - *Supplemental guidance for applications*

FAA Legislation

The FAA-AST Legislation is under the United States Code (USC) Title 49, Subtitle IX, Chapter 701[18] and details the launch licensing requirements at the top level.

FAA Regulations

The FAA-AST Regulations for commercial spaceflight are contained within the Code of Federal Regulations (CFR) Title 14 Chapter III [21]. The scope covers the procedures and requirements for commercial space transportation activities.

2.3.2 FAA Safety Regulatory Review & Gap Analysis

This section provides a review of the FAA-AST safety-related documents governing the early phase of Test & Evaluation and also Operations. The review is based on whether the FAA-AST guidelines are effective in that they have a rationalised approach and whether the approach would be suitable for European operations; where this is not the case it is identified as a gap. These gaps would then form the basis from which to research the area in conjunction with the 'safety tools and techniques' section (1.5.4) in order to derive a proposed suitable method for European operations and possibly for other bodies to consider (such as the International Association for the Advancement of Space Safety in Chapter 3.1).

Review of FAA-AST Hazard Analysis Guidelines

The main documents driving safety activities are the FAA AST Advisory Circular AC437.55-1 [18] and the System Safety Process AC431-35-2A [61] and these are summarised here.

Hazard Analysis Guidelines under an Experimental Permit (AC437-55-1)

It is not clear to whom the guide applies to i.e. designer and/or operator because the guidelines refer to the 'operator' per CFR 401. Within CFR 401, the term Operator means '*a holder of a license or permit under 49 U.S.C. Subtitle IX, chapter 701.'* So if we take the case of Space Ship 2 this is being designed and tested by Scaled Composites and will be operated by Virgin Galactic. It is assumed that the guideline means Scaled Composites in this instance because they will hold the experimental license. Should this be the case we are really talking about the design organisation with their systems safety analysis that then uses their own test pilots to fly (operate) during tests.

The AC (along with all FAA-AST regulations and guidelines) is concerned with '*protecting the public'* only. This is commendable however it is clearly more biased towards the orbital aspects with flight trajectories (launch and re-entry) that clearly overfly populated areas and with expendable propulsion tanks (solid rocket boosters for instance) on the ascent and during re-entry are travelling at high Mach numbers with possible damage due to space debris, etc. and so could break up. This should not be a factor at all for suborbital flights that take-off (launch) from point A and return to point A; all of which will be in a defined and unpopulated corridor. So in terms of protecting the public for suborbital flights this aspect should not be a driving factor in the analysis; though it clearly is for the FAA-AST as they mandate that the Expected Casualty (Ec) analysis is conducted for commercial spaceflight (see further below for Ec discussions).

[18] http://www.faa.gov/about/office_org/headquarters_offices/ast/regulations/

This is the main weakness in the FAA-AST approach: it is a one-shop approach that covers orbital and suborbital flights and the author contends that the differences are too great and that the different domains should be split out with proper and rationalised regulations and guidelines for each.

At least for the hazard analysis guidelines (AC) it does specify suborbital in the title and so the rest of this review shall focus on these aspects.

The AC provides a (too) simplistic hazard analysis process:

(a) Identify and describe the hazards

(b) Determine and assess the risk of each hazard

(c) Identify and describe risk elimination and mitigation

(d) Validate & Verify risk elimination and mitigation measures

FAA-AST mandates a level of safety in the technology of Reusable Launch Vehicles (RLV's) through its permit and licensing process. The AC details that '*public*' hazards identified as 'Hazardous' or 'Catastrophic' must be mitigated to reduce the severity of their impact, or be proven through design to have a likelihood of occurrence of either Remote or Extremely Remote (with a chance of occurrence of less than 1 in a million), in order to be acceptable for permitting or licensing.

AC 437.55-1 [18] defines the 'Acceptable Level of Risk' to protect public safety and the different Hazard Severity and Hazard Likelihood categories used to determine the level of risk.

The FAA does not mandate any level of acceptable risk for passengers. The FAA allows passengers to fly at their own risk and requires only that they are informed of the risk they are taking, by the spaceflight Operator. The FAA does mandate an acceptable level of risk for the crew. As part of the FAA's requirement to protect public safety, they mandate that the crew must be able to control a Reusable Launch Vehicle (RLV) and be capable of acting in emergency scenarios. Crew actions and RLV operability are covered in the hazard analyses that a 'permitee' and licensee must supply and show compliance with the FAA acceptability matrix in order to be approved for operation.

FAA-AST AC 437.55-1 Probability Classifications: These are calibrated such that the catastrophic/extremely remote 'safety objective' is $1x10^{-6}$ per mission and there is no clarification on why this value was chosen; in particular when their orbital industry uses the Expected Casualty 9Ec) target of $30x10^{-6}$ per mission. This is clearly 30 times worse than the 'safety objective' proposed below and equates to $0.3x10^{-4}$ per mission. Then the 'occasional' classification cell is two orders of magnitude (whereas the others are singular); this is not rational and also the term 'extremely remote' is not in accord with the best practice methods.

What does this mean in terms of understanding the cumulative risk from the safety objective of $1x10^{-6}$ per mission for catastrophic failures? The AC does not even mention this and here is a clear lack of understanding between hazard probability and overall risk. It actually means that, due to circa 100 critical failures, that the target is $1x10^{-4}$ and 10% of accidents are due to safety critical systems (90% due human error and structural aspects) then the target is $1x10^{-3}$ per mission. This accords with the orbital industry thoughts (such as in the IAASS-ISSB Space Safety Standards Manual [16]); but there they suggest that the suborbital domain target should be an order of magnitude better at $1x10^{-4}$. There is another clear indication that the criterion is different and so are many other considerations.

DESCRIPTION	LEVEL	INDIVIDUAL ITEM
Frequent	A	Likely to occur often in the life of an item, with a likelihood of occurrence greater than 10^{-2} in any one mission.
Probable	B	Will occur several times in the life of an item, with a likelihood of occurrence less than 10^{-2} but greater than 10^{-3} in any one mission.
Occasional	C	Likely to occur sometime in the life of an item, with a likelihood of occurrence less than 10^{-3} but greater than 10^{-5} in any one mission.
Remote	D	Unlikely but possible to occur in the life of an item, with a likelihood of occurrence less than 10^{-5} but greater than 10^{-6} in any one mission.
Extremely Remote	E	So unlikely, it can be assumed occurrence may not be experienced, with a likelihood of occurrence less than 10^{-6} in any one mission.

Figure 33: FAA-AST AC 437.55-1 Probability Classifications

Severity Categorisations: As can be seen in Figure 34 the focus for severity classifications is on the '*public*'; there is no mention of the crew or passengers (SFPs).

DESCRIPTION	CATEGORY	CONSEQUENCE DEFINITION
Catastrophic	I	Death or serious injury to the public.
Critical	II	Major property damage to the public, major safety-critical system damage or reduced capability, significant reduction in safety margins, or significant increase in crew workload.
Marginal	III	Minor injury to the public or minor safety-critical damage.
Negligible	IV	Not serious enough to cause injury to the public or safety-critical system damage.

Figure 34: FAA-AST AC 437.55-1 Hazard Severity Classifications

FAA-AST AC 437.55-1 Risk Matrix is at Figure 35 below. This, like the §23.1309 is based on a single line (Go or No-Go approach) which is acceptable to demonstrate that a hazard's probability (failure condition in §23.1309 terms) is met, depending on the severity classification. Step (b) above suggests that the operator (designer) should then determine and assess the risk for each hazard; this is where the problem arises. In §23.1309 there is no Risk Assessment or Risk Assessment Matrix, the designer must meet the specified safety objective for a failure condition hence they have a 'single line' reflecting the catastrophic/extremely improbable objective for instance. Here the FAA-AST has attempted to revert to the risk granularity methodology but then have kept the single line approach; this is even done poorly because as depicted below it states that it is acceptable to have Frequent/Marginal risks. It is considered that this 'mix-up' in strategy is based on the earlier Re-usable Launch and Re-entry Vehicle System Safety Process [61] in 2005 whereby the Risk Acceptability Matrix did include margins for risk (as opposed to meeting a safety objective) and Figure 36 further below shows the 'medium' tolerability band as well as the unacceptable (high risk) and acceptable (low) risk bands. Here by having an order of magnitude between the unacceptable and the acceptable allows the 'operator' tolerability of risk (as opposed to definitive safety objectives). Arguably with 100 failure conditions there should be two orders of magnitude between the unacceptable and acceptable boundaries; hence rationale could have been applied and explained.

Severity / Likelihood	Catastrophic I	Critical II	Marginal III	Negligible IV
Frequent (A)	1	3	7	13
Probable (B)	2	5	9	16
Occasional (C)	4	6	11	18
Remote (D)	8	10	14	19
Extremely Remote (E)	12	15	17	20

Figure 35: FAA-AST AC 437.55-1 Risk Matrix

Severity / Frequency	Catastrophic I	Critical II	Marginal III	Negligible IV
Frequent (A)	1	3	7	13
Probable (B)	2	5	9	16
Occasional (C)	4	6	11	18
Remote (D)	8	10	14	19
Improbable (E)	12	15	17	20

Level	Index	Hazard Risk Acceptability Criteria
High	1 - 6	Corrective/controlling actions must be taken to reduce the hazard severity below "II" or reduce the likelihood of occurrence below "C".
Medium	7 - 10	If not controlled, the risk must be accepted by Program Management and FAA.
Low	11 - 20	Project Management decides on actions, if any.

Figure 36: FAA-AST AC431.35-2A Hazard Risk Index matrix

Step (c) further above in the hazard analysis guideline is to '*Identify and describe risk elimination and mitigation'*. It then goes on to say that '*the first priority should be to eliminate the hazard*.' A hazard has a likelihood (probability) property and does not have risk i.e. both likelihood and severity. A hazard can lead to different accidents and therefore have different outcomes (or consequences); hence the risk (severity and probability) is associated with the accident and not the hazard. This may be semantics but it is important to establish the basic premise of ones methods otherwise the result is confusion as per the FAA-AST because in one breath they were talking about Hazard Risk Acceptability Criteria and then in the next breath talking about just Risk Acceptability Matrix. Also in both they have left in the indices whereas in §23.1309 there are no such indices; merely a Go-No-go line as to whether your **probability** has met its safety objective or not i.e. there is no mention of risk.

Section 7.0 mentions acceptable analytical approaches (PHA, FMEA/FMECA and FHA) but should also state that other diverse methods should also be included as per ARP 4761 for example; including OHHA, OSHA, ZHA and PRA (one would assume that PRAs would be required for the Rocket Propulsion System as this is the most problematic in proving and meeting safety objectives). Also

within the 'additional considerations' under 'training' it states that '*Designing safety into the system requires that personnel involved in system development, production and operation understand and practice operations and procedures that protect public safety'*. Once again, the FAA-AST is only concerned with 'public safety'. Additionally they state '*Training can help ensure that personnel produce a safe system or operation'*; for both of these points under 'Safety Training' the key terms are 'understand and practice operations and procedures' – however the focus should be twofold; Safety Management awareness training for all company members and specific SMS training for key-post personnel (the Safety Manager/Ops Manager/Company President, etc. – i.e. to all personnel with direct responsibility for the Go/No-Go or Flight Readiness review process). This is a vital component of an SMS and should be instigated as early as possible; a safety culture ensconced throughout the company leads to a 'generative culture'. Saying 'Safety is our Number One Priority' when you do not have a qualified and competent Safety Manager and no SMS in place can actually be detrimental in the end (training and defined competencies can be a mitigation event in order to reduce the likelihood of an accident occurring).

Section 8 covers the abort criteria: A dedicated flight safety system (FSS – see definitions Table 1) could protect the **public and property** from harm by terminating powered flight of a vehicle that does not stay on its intended course (to maintain the Instantaneous Impact Point [IIP] within its operating area. Arguably the analysis should consider both the people on board and the people (and property) on the ground and therefore if terminating the thrust is an option then this should be employed - this should not mean a total flight termination (destruction).

A good point of the guideline is that in section 9.0 it states that '*to obtain a re-usable launch vehicle* (mission) *license* (following on from an experimental license), *an operator must employ a comprehensive system safety program plan consisting of both system safety management and system safety engineering*.' It then suggest that as well as the analysis undertaken in accordance with the AC, that a system safety process should be employed as detailed in Re-usable Launch and Re-entry Vehicle System Safety Process [61] and including:

- *Inclusion of a safety organization*
- *Designation of a safety official*
- *Development of a system safety program plan*
- *Identification of safety-critical systems and events*
- *Documentation of systems and sub-systems hazard analyses and risk assessments*

As opposed to obtaining an experimental permit (for Scaled Composites) to obtain a launch mission license will be the responsibility of the operator (in this sense it will mean the operator as Virgin Galactic) and this makes sense for some of the bullet points above such as a safety official and organization but it is the responsibility of the design organisation (Scaled Composites) to undertake the sub-system and system hazard analysis i.e. systems safety engineering and it is up to the operator (Virgin Galactic) to undertake system safety management, including operator safety risk management. Once again the AC is confusing the terms and only has one term for 'operator' which can have two meanings. This stems from the orbital launch domain because in the aircraft domain (and in the suborbital domain) a design organisation such as Scaled Composites will then hand the aircraft/spacecraft over to the operator such as Virgin Galactic (orbital companies such as Space X will design and operate the vehicle so the terms and analyses is more biased to that domain).

System Safety Process AC431-35-2A

This AC is a high-level guide to the FAA-AST safety process and once again the focus is on the '*public*'. The document contains the FAA-AST three-pronged strategy '*to ensure public health and safety and safety of property*' as depicted in Figure 37.

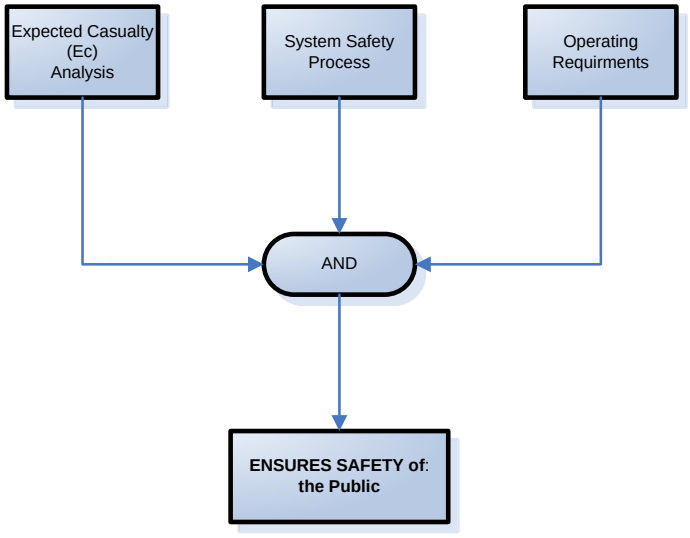


Figure 37: FAA-AST 3-pronged strategy to assure 'Public' safety

The document once again refers to the 'operator' as described in the previous section and this is biased towards orbital companies and within the suborbital domain it is arguably a mix between the designer in the first instance (for obtaining an experimental permit) and then for the operator in obtaining a mission license. As can be seen the middle portion of the 2 interdependent prongs is the system safety process. This is the standard design process backed up by systems safety analysis. Within this prong the designer will undertake standard systems safety engineering at sub-system and system level, identification of safety-critical items and the safety V&V process. The document provides useful guidance and then amplifies the AC 437-55.1 aspects and also describes the system safety program plan elements. Figure 2 of the document presents a good diagram depicting the System Safety Engineering Process Flow. As it addresses safety-critical scenarios and events it also includes flight trajectory analysis and in the case of SoA this is an important factor. Arguably the flight will be contained within a NOTAM special SoA area but nonetheless analysis should be undertaken as to non-nominal trajectories and the likelihood of causing a 3rd party death(s) (the public). Section 6b(2) suggests that safety critical systems may or may not be critical at all times of the flight i.e. the ability of the flight path to reach populated areas. It is considered that even in remote areas a safety critical failure could affect the people on board (and/or the vehicle) and should be considered within the analysis for European operations.
Figures 3 & 4 represent good diagrams for hazard identification and analysis, including for System and Sub-System Hazard Analysis and details acceptable tools and methods. Section 6b (3) (i) covers the standard safety precedence for eliminating or mitigating risk and section 6b (3) iv covers two specific risk mitigation measures; the FSS and the NOTAM/Notification to Mariners area.

The left prong from Figure 36 concerns the Ec analysis and this is examined further below.

The right prong concerns 'operating requirements' and these concerns '*the operator's ability to operate within the limits of acceptable risk to public safety*.' Essentially these are operating procedures and limitations required (at the operator level and not design level) and the document provides examples of these:

- *Launch commit criteria and rules*
- *Human activation or initiation of a Flight Termination System to initiate safe abort during launch and re-entry*
- *System monitoring, inspection and checkout procedures*
- *Inspection and maintenance for re-flight*
- *Selection of primary and alternate landing sites for vehicle or stages*
- *Surveillance and control of landing areas*
- *Standard limits on weather*
- *Co-ordination with appropriate airspace authorities*
- *Limits on flight regime (ties in with analysis, testing and demonstrating confidence in system performance and reliability)*
- *Regulatory limits on flights over populated areas*

As can be seen it is the operator (Virgin Galactic in the example) who is to undertake the left and right prongs of the FAA-AST strategy and the designer (Scaled Composites) who undertake the core central prong. This vilifies the author's safety model in that the operator safety risk management is where the operating procedures and limitations are managed; however the document is biased towards the orbital domain in that it presumes the 'operator' is one and the same organization i.e. both designer and operator are the same company such as Space-X.

The document provides an example SSPP which covers all of the points in the main document in a template form and with examples of Risk (Hazard) Reports; this is an indication that clearly shows the lack of a joined up approach for Designers and Operators and lack of understanding of hazards and accidents i.e. the first example has a hazard as 'primary load structural failure: vehicle airframe failure' and then in the details of the hazard description says 'consider wings, booms, stabilizers' and the effect is 'loss of control, loss of vehicle'. Hence they are mixing up the ICAO Accident 'Structural Failure' with the ICAO Accident 'Loss of Control'; for instance by separating the failure conditions properly one would then be able to link those to the relevant accident; in this case a stabiliser failure would more credibly lead to a 'Loss of Control' Accident, as opposed to a failure condition of 'primary structure failure' which leads to the Accident 'Structural Failure'

Review of CFR Part 417 – Launch Safety

The FAA-AST has based a lot of their Licensing Rules on the legacy requirements from the vertical launches undertaken by NASA and hence the main focus is protection of the 'public'. The definition of 'public' can be found in the CFR Part 401 [21] and public safety is defined as:

Public safety means, for a particular licensed launch, the safety of people and property that are not involved in supporting the launch and includes those people and property that may be located within the boundary of a launch site, such as visitors, individuals providing goods or services not related to launch processing or flight, and any other launch operator and its personnel.

As per CFR Part 417 [22] the FAA-AST requires Expected Casualty (Ec) Analysis to be undertaken in order to demonstrate that an RLV meets the Ec target ($30x10^{-6}$ risk of general public fatalities).

This analysis will account for the following items:

- *Regions of land, sea, and air potentially exposed to debris resulting from normal flight events and from potential malfunctions.*
- *Waterborne vessels or aircraft exposed to debris from events resulting from potential normal or abnormal flight events, including vehicle malfunction.*

- *Operational controls implemented to control risk to the public from debris hazards.*
- *Debris identified from debris analysis.*
- *Vehicle trajectory dispersion effects in the surface impact domain.*

The Ec is further discussed below in 'Review of FAA-AST Safety Critical Hardware Guidelines'.

Review of Part 460 – Human Spaceflight Requirements

The FAA-AST has provided Human Spaceflight Requirements and these are covered further below in Section 2.3.4 and 2.3.6 for flight crew and Spaceflight Participant requirements. Additionally a review of NASA and ESA Human Rating Requirements is covered in 2.3.11.3.

Review of FAA-AST Validation & Verification Process

The FAA-AST has provided a safety validation and verification guide [62] to act as a companion to their system safety process guide [61] in order to provide relevant information to support a Launch License application. A review of the guide concludes that the document is a high-level reiteration of standard practices such as ARP 4751 and does not provide any new methodology for the emerging commercial spaceflight industry. In its scope it states that "*the specific content of the V&V process exceeds the scope of this guide*."

Review of FAA-AST Safety Critical Hardware Guidelines

The FAA-AST guideline on the identification of safety-critical items [63] is a reasonable attempt at providing specific guidance for RLV developers.

The guidelines suggest that risk assessments are specifically conducted for:

- *Expected Casualty (Ec)Analysis*
- *Instantaneous Impact Point (IIP) Analysis*
- *IIP Trace Analysis*
- *Dwell Time*
- *Population Density*
- *Casualty Area*

They categorise the hazard contributors into the following categories:

- *Safety-critical hardware*
- *Safety-critical software functions*
- *Safety-critical procedures*

The guidelines further define what is considered a safety-critical item and that the activity should be conducted separately from the structured risk assessment process. They suggest that if BOTH of the following conditions are true then the item is potentially safety critical and may require further analysis:

- *If the vehicle is over/in a populated area, or may reach a populated area as a result of failure and*
- *The system could credibly fail, with the failure resulting in one or more of the conditions below;*

- *Failure causes break-up*
- *Failure causes loss of control*
- *Failure causes uncontrolled debris*
- *Failure causes uncontrolled discharge of hazardous material*
- *Failure prohibits safe landing*

The guideline is the standard way of providing safe assurance of '*protecting the public'* and the aim is to meet the Ec requirement of $30x10^{-6}$ per mission and determine whether safety-critical items are identified and therefore to list these in support of the Launch License application. Herein lays one of the issues of this approach; if the applicant proves that their analysis is better than the $30x10^{-6}$ requirement (due to their flight trajectory not impinging too much on the public) then they need not identify safety-critical items. The guideline states (paragraph 7.3 – safety critical assessment, item 5a) "*Perform a preliminary risk assessment* (on the potentially safety-critical item). *If it meets the allowable criteria, no further analysis may be required*."

Additionally the 'target' (requirement) of *$30x10^{-6}$ per mission* stems from the standard industry practice from the orbital-based missions. A more accurate way of presenting this is either $3x10^{-5}$ or actually $0.4x10^{-4}$ per mission; clearly a low target which is based on previous occurrences from within the 'Space Shuttle' and rocket industry. Within today's commercial spaceflight industry we have simpler designs and less exacting environment for the suborbital vehicles; it is acknowledged that for orbital commercial operations then following the existing requirements would be acceptable until more data is obtained in terms of reliability. However suborbital operations should have more rationalised criteria and targets and therefore safety-critical items would be listed and managed (as per current aerospace requirements) irrespective of whether an item meets the target i.e. within proper safety analysis a safety-critical item may have a better reliability value than the target but is still analysed as part of its contribution to the accident (such as a catastrophic failure condition).

Review of FAA-AST Software Safety

The FAA-AST has provided a software safety and computing system guide [64]. By computing system they mean computer system hardware and firmware. The guide states that *the majority of software problems can be traced to improper design or improper implementation if that design….Therefore the software and computing system safety should focus on the fault avoidance, removal, detection, and tolerance*. This is good guidance but should also state at this high-level introduction to include fault tolerance i.e. the software/computing system safety effort is required to be joined up with the main safety effort because it should be stated within the software safety requirements that should a system fail due to software then the tolerance of the system should not result in a catastrophic outcome.

The guide follows best practice in that it covers the main topics as covered in 2.2.4.2 such as:

- *Software safety planning*
- *Safety Critical Computer System Function Identification and Description*
- *Hazard analyses*
- *Standard Risk Mitigation Measures – here in the detail the document finally mentions software fault tolerance*
- *Validation & Verification*
- *Additional considerations;*
  - *Development Standards*
  - *Configuration Management and Control*

- *Quality Assurance*
- *Anomaly reporting*
- *Training*
- *Maintenance*

- *Lessons Learned*; this section provides a list of broad lessons from a study of accidents involving software and computing systems.
- One of the key Lessons Learned appears to be 'estimating and mitigating risks are critical aspects of software safety'.

The Appendices are useful covering 'generic software safety requirements' (Appendix A), software and computing systems hazard analyses (B) and finally the space vehicle failures and aircraft accidents (C).

Overall the guide is very good and the only important missing aspect is consideration to the Design Assurance Levels (DALs) i.e. from the DO-178B standard and also for the computing systems DO-254 regarding complex hardware. It is considered that this is a key factor in the integration of the software safety effort to the main system safety effort.

Review of FAA-AST Operations & Maintenance Guidelines

The FAA-AST has provided Operations and Maintenance guidelines and with all of their documents the scope covers both orbital and suborbital RLVs. The guide provides a useful set of statements for maintenance and operations that could be interpreted as requirements (*the applicant should have .....)* and this is backed up with a '*rationale*' paragraph. The sections covered include; RLV Maintenance, RLV Support Personnel and RLV Operations.

RLV Maintenance

This section focuses on the fact that an applicant should have a maintenance program plan and maintenance inspection schedules and an accompanying Configuration Management System. These are all very generic as one would apply to any program and it is not only until in section 6.7 does it reflects Re-Launch Vehicles stating that:

> *"The FAA expects that initially flights will have many systems or components that are inspected after every flight. Once sufficient experience exists to determine the reliability of various components, subsystems, and systems, the applicant should update its inspection schedule. An up-to-date inspection schedule will ensure that the applicant has a well-documented inspection plan based on the design and operation of the RLV that contributes to public safety and meets the operational needs of the RLV developer"*

In this respect more guidelines are required and in particular regarding Composite Materials and reusable Rocket Propulsion Systems (including hybrid technologies).

RLV Support Personnel

This section relates to suggested various roles of support personnel and also that operators should have a training plan for these personnel. This is standard information and operators may wish to refer to the guidance but it is not considered exceptional in terms of specific RLV/SoA guidance for operators.

RLV Operations

This section relates to '*operations*' and therefore one would expect to see guidance on the operational aspects in terms of operating profiles, flight crew issues and so on. In fact the guidance is mainly for designers on design aspects for operating the vehicle within its design limitations and with intent of usage; example of this include sections on 'systems engineering', 'electrical power-system' and 'structures' (…*the vehicle structure should be designed to preclude failure by use of adequate safety factors* …). There are a few specific 'requirements' to operators such as use of communications but these are standard procedures.

Summary

Once again the guidance is to '*protect the public'* and therefore assuming there will be a trajectory over a populated area; in suborbital flights there should be a remote excluded zone for initiating the Rocket and this should not be a factor – essentially this is aimed at the orbital domain.

Also there is no mention of maintenance/operations human error and management thereof and one would expect this to be included i.e. maintenance error management systems, including reporting of incidents and also the same for flight crews in reporting air/space incidents.

2.3.3 Conclusion of FAA Safety Review

The Gap Analysis of the current state of the Industry clearly concludes that the Rules & Guidance are still immature and of concern is that they are not robust. Although the FAA want to allow Designers and Operators 'flexibility' and do not want to 'stifle' the Industry's growth by imposing too restrictive regulations, standards must be established that are clear and robust, whilst at the same time be pragmatic. The main areas of concern can be summarised as follows:

- Poorly defined Safety Criteria
- No Accident List
- No Safety Targets
- No Hazard Risk Budget
- Guidelines are for 'operator' – currently meaning the design organisation applying for a launch license for their test flights; what about guidelines for the operator meaning Virgin Galactic for instance

It is clear that the FAA-AST Rules and Guidelines are for the 'Experimental' Launch License applicants and that the major mitigation is the remoteness of the Launch site i.e. Virgin Galactic/Scaled Composites will 'launch' their SS2 over the Mojave desert. In Kemp's book [15] regarding the aforementioned he quotes Burt Rutan speaking to the House of Representatives Space and Aeronautics Subcommittee about the FAA-AST process:

> *'The process deals primarily with the consequence of failure, whereas the aircraft regulatory process deals with reducing the probability of failure'*

This statement echoes the author's views from and the FAA-AST's approach remains the same today. It is interesting that Burt Rutan's comments imply that the FAA-AST should be looking at the aircraft regulatory process i.e. certification approach, as opposed to the Launch Licensing approach; this seems to have fell upon 'deaf-ears' which is a shame because of Burt Rutan's experience in aerospace and now space.

The safety guidelines are meant for the Design Organisation however they do refer to actions that the Operator should do; it is considered that the guidelines are not appropriate for operators and they are also not specific enough for DOs. Furthermore they do indeed focus on the consequence of failure to

the ‘public’ rather than the bigger picture of risk reduction of the vehicle to protect all parties involved.

These issues are discussed in Chapter 3 with proposed solutions presented for Industry consideration.

2.3.4 FAA Regulatory Medical Review & Gap Analysis

The main reason for the FAA regulators stipulating minimum medical requirements is the additional hazards inherent in the space environment. As detailed in the author’s Thesis on safety of the customer [65], the space participant (SFP) will be subject to acceleration forces in the region of 3 to 5G and also micro gravity for up to 5 minutes. These forces could aggravate medical conditions in SFPs, which could result in an in-flight medical emergency or death (not only is this undesirable for the individual, it could compromise the crew and/or other participants in their duties or in their health). The medical concerns for suborbital spaceflight as a result of the relatively high G-forces include:

- Neurovestibular – this is most likely in the +Gz or ‘eyeballs down’ acceleration; hence seat design should be angled back so that the person feels the acceleration more in the +Gx plane (chest to back) as the body can generally withstand a higher level of ‘G’. These acceleration forces, coupled with noise and vibration may also induce motion sickness.
- Cardiovascular – changes in cardiac rate and function which could lead to a heart attack.
- Musculoskeletal – neck injuries are most likely when experiencing high G-forces.
- Pulmonary Function issues – difficulty with breathing due to airway closure or pressure on the lungs (the author experienced this during Gx centrifuge experiences).

Additional environmental issues to consider include:

- Noise – the rocket engine will transmit the noise through the cabin and therefore headsets or helmets will be required (certainly by the crew, but as a duty of care will also be required for the SFPs). Table 3 in the author’s Thesis [65] assumed the maximum SoA/spacecraft noise to be 95dBA and the minimum time (15 minutes was the minimum time in the table) which resulted in a resultant noise exposure of 80 dBA; the rocket phase will only be up to 90 seconds for the Virgin Galactic vehicle and therefore this should not pose a major issue for SFPs (apart from adding to Space Motion Sickness) however flight crew’s performance may be affected.
- Vibration – the video footage of Spaceship One’s X-prize winning flights highlights a vibration issue in the rocket phase of the flight; once again this will only be for up to 90 seconds however this is more of an issue than noise. The reason is that vibration can impair the pilot’s performance to track displays and maintain situational awareness.
- Radiation – the author’s Thesis [65] concluded that radiation should not present a major issue for suborbital flights for SFPs but flight crew could be susceptible to the effects of radiation over a long period; it was detailed that suborbital pilots would be exposed to less amounts (suggested 7-15mSv [Sievert] annual exposure) than that experienced by NASA crews and also Nuclear Radiation workers. An annual and career limit was also suggested.
- Flight Emergencies (fire/smoke, decompression, non-nominal loss of control or spins) – various flight emergencies could occur and result in the crew and SFPs being exposed to differing situations with medical implications.

The overarching FAA guidance for medical criteria is contained within [71] and the following Gap Analysis regarding flight crew and participant medical standards is from the Draft FAA guidelines as detailed below.

Flight Crew Medical Requirements

The flight crew standards concerning medical criteria are defined in CFR 460 'Human Spaceflight Requirements' [71] and also in draft guidelines [67].

These state that:

> *'The FAA's Office of Aerospace Medicine (AAM), which includes the Civil Aerospace Medical Institute (CAMI), the medical certification, research, and education wing of the AAM, considers the medical qualification standards for 2ndclass airman certification to be adequate standards for RLV flight crew on a suborbital launch due to its inherently short duration'.*

This is considered one of the FAA-AST's flexible approaches in that it does not have too prescriptive requirements so as not to stifle the industry. This is commendable but only to a point. There are certain aspects that require specific rationale or pragmatism or indeed common sense. In the case of flight crew only needing a Class II aeromedical certificate is a case in point. The counterargument is that the requirement should be more restrictive and hence a Class I aerospace certificate should be the required standard; this is corroborated further below in aerospace medical working groups.

Spaceflight Participant Requirements

In terms of the SFPs the FAA-AST requirements [66] state that:

> *'Each space flight participant should provide his or her medical history to a physician experienced or trained in the concepts of aerospace medicine. The physician should determine whether the space flight participant should undergo an appropriate physical examination.'*

This may seem reasonable but this does not provide useful guidelines and leaves the operator to determine what medical conditions would be acceptable; also no there are no guidelines as to what age is acceptable and what weight limit is acceptable for instance; these aspects are important to derive in the beginning and arguably they can then be relaxed as more knowledge is gained after a predetermined amount of data has been examined by the experts. Additionally there is currently no official 'Go/No-Go' list of conditions that may contraindicate a SFP from participating in a suborbital flight. Various working groups in the USA and EASA should leverage any good work done thus far and using a European-based working group could provide more positive guidelines.

The analysis reflects a flexible approach from the FAA-AST in that they do not want to prohibit people from flying unnecessarily and tends to place the responsibility onto operators. However some operators may follow the guidelines precisely whereas others may include excessive medical standards that would exclude many of the prospective SFP. Also there has been no thought given to anthropometrics involved; for instance are they assuming that the SFPs will all be within the 5% – 95% size range? Also what about age restrictions or weight limitations?

Medical Papers/Reports

There are a number of papers and reports on approaches to take for suborbital spaceflight and also raising pertinent debate on specific medical 'conditions' that may be acceptable or not.

The author was privileged to partake in a Virgin Galactic Medical Panel where medical conditions such as false breasts (as one of their SFP has implants). More genuine concerns included whether heart pacemakers could be allowed and about general operations and healing time before flights. A paper on Emergency Medicine for Human Suborbital Spaceflights [68] queried conditions such as pregnancy and SFP's psychological conditioning.

The author presented a co-authored paper at the 3rd International Association for the Advancement of Space Safety (IAASS) [70] including discussions on medical criterion:

Minimum medical fitness requirements are likely to comprise an in depth medical and lifestyle questionnaire, consultation with the participant's general practitioner, clinical examination, 12 lead ECG, lung function testing, blood and urine analysis and blood pressure measurement. With these tests regarded as the basic standard screening, additional tests would be undertaken dependent upon the results from standard screening and the spaceflight participant's age, with older participants subjected to increased scrutiny. The aim should always be to optimise the amount of medical screening performed in line with current knowledge.

Another paper on Suborbital Commercial Spaceflight Crewmember medical issues [69] also proposed more stringent and explicit medical and training requirements (though just concentrating on flight crew). The paper was produced from the efforts of aerospace medical experts in conjunction with industry companies such as XCOR and Blue Origin and included personnel from NASA, the FAA-AST and notably the Virgin Galactic Chief Medical Officer (and former Wyle Aerospace Physician) Jim Vanderploeg. The paper also highlights the shortfall in FAA-AST policy, stating that '*policy and decision processes to be used for waivers and what functional tests (centrifuge, parabolic flight, altitude chamber) will be required to demonstrate that an individual can perform in the suborbital environment is still undefined by the FAA*.' The paper uses the Virgin Galactic flight profile as the model from which to base their working group discussions and concentrated on the following '*medical risks*':

- Acceleration; here the discussions concentrate on the different types and levels of 'G' expected in the flight profile and notably makes a comparison of fighter jet profiles in a common phenomenon called the 'push-pull effect' – this is whereby a pilot experiences –Gz (such as when flying an outside loop) and then manoeuvres into a +Gz state which could result in 'G-Loss of Consciousness' (G-LOC). The paper states that this phenomenon has been implicated in several combat training fatalities. The relevance here is that at the apogee of the flight profile the flight crew may experience –Gz whilst upside down during the microgravity phase and then during the re-entry (descent) phase may transition to +Gz (and or +Gx) therefore the 'push-pull effect' may be an issue. Although G-LOC may not frequently occur a more likely outcome could be Almost Loss of Consciousness (A-LOC) resulting in impaired cognitive performance; this may be a frequent event during the 'push-pull effect' of transitioning between microgravity and the descent.
- Microgravity Effects; here the paper suggests that it is possible that inexperienced, non-adapted, or overly sensitive individuals might experience symptoms (neurovestibular or cardiovascular) associated with even short exposures to the space environment.

- Cardiovascular Effects; here the discussions concentrate on the Space Shuttle astronauts and state that the effects should be minimal for suborbital flights. However the suggest that '*although post-flight orthostatic hypotension should be minimal on suborbital flights, the risk of orthostatic hypotension during entry may be quite real. The enhanced parasympathetic tone that occurs after several seconds of exposure to –Gz leads to bradycardia, diminished cardiac contractility, and peripheral vasodilatation. This response increases the risk of a fall in head-level blood pressure on re-exposure to +Gz. A full compensatory response can take 8 to 10 seconds with the recovery period dependent on both duration and magnitude of relative –Gz. Given that the period of hypoxia latency for brain cells is 4 to 6 seconds, the risk for +Gz related symptoms is enhanced at lower than expected +Gz levels*'
- Neurovestibular Effects; here the paper suggests that neurovestibular issues are not considered a significant factor in that the exposure to microgravity will be less than five minutes duration for each suborbital flight. Neurovestibular dysfunction after orbital flight includes an altered ability to sense tilt and roll, defects in postural stability, impaired gaze control, and changes in sensory integration.
- Space Motion Sickness; Microgravity exposure results in space motion sickness in about 70% of astronauts flying on orbital space flights for the first time. It is thought to be due to a sensory conflict between visual, vestibular, and proprioceptive stimuli. Susceptibility cannot be predicted by susceptibility to ground-based motion sickness or pre-flight testing. Symptoms typically occur within the first 24 hrs. However, symptoms have been reported immediately after main engine cut off with dizziness, pallor, sweating, and severe nausea and vomiting. Vomiting can crescendo quite suddenly without any prodromal symptoms. In a multi-passenger vehicle, one passenger becoming nauseated can potentially trigger nausea in the other vehicle occupants. Essentially it is not anticipated to be a major concern for the flight crew but some SFPs may be more susceptible than others and vomit may be an issue that could 'float' forward to the cockpit area and possibly affect the flight crew's performance.
- Post-Flight Medical Problems: it is not anticipated that any major issues will exist for suborbital flight crew (however some SFPs may be affected by the flight)
- Entry Motion Sickness; this is really for orbital crews returning to the Earth's gravity and should not be a factor for suborbital flights.
- Emergency Egress Capability; it was noted that 5 to 15% of orbital crews suffered from one of the conditions mentioned above and were judged too impaired post-landing to perform emergency egress (unaided). This is not considered an issue for suborbital flight crew.
- Spacecraft Cabin Environment; the paper suggests that without a pressure suit the crew is absolutely reliant on cabin integrity being maintained as there is no redundancy and depressurization would be a catastrophic event. Additionally the atmosphere composition (O_2 and CO_2) would need to be controlled within safe levels so as not to impact performance.
- Ionizing Radiation; the paper suggests for the most part, there is no concern regarding the acute effects of ionizing radiation because of the short duration of the flight and the fact that launch can be controlled depending upon atmospheric conditions.
- Noise; The physiological effects of extreme acute noise (unprotected) is reduced visual acuity, vertigo, nausea, disorientation, ear pain, headache, temporary hearing thresh-hold shift, and degradation in pilot performance. Loud noise can also interfere with normal speech, making it difficult to understand verbal communication and affecting team interaction.

- Vibration; Vibration was also noted on the in-cabin videos of several of the Spaceship One flights during both ascent and entry. Spaceship One Flight 16P experienced significant thrust oscillations at 5-10 Hz towards the end of the two phase flow portion of the boost which produced an impressive amount of vibration with the pilot's head being slammed against his headrest for several seconds as seen on the in-cabin video.

The issues discussed and the medical recommendations have an impact on the safety effort in a positive sense i.e. they are actually controls to hazards or accidents and so these have been extracted as such and discussed in Chapter 3.6.

2.3.5 Medical Review Conclusions

The FAA has once again adopted the 'flexible' approach by not imposing strict medical criteria for the flight crew and participants. The main areas of concern are as follows:

- Flight Crew Medical Criteria – Category 2 only
- SFP Medical Criteria – Basic Medical Questionnaire and General Practitioner Medical only
- No guide as to medical issues to be addressed

The Medical community are clearly experts in their field and are asking the right questions and providing useful guidelines to provide a 'Go/No-Go' medical standard; though it is also clear that the 'Grey' area conditions require further research. However the Medical community may not appreciate the full extent as to why these Medical criteria are important in terms of safety mitigation against Inherent 'Accidents' within the accident sequence.

It is concluded that the FAA have provided criteria that is not sufficiently robust and that having too flexible an approach may be detrimental in that some operators may follow the 'unrestrictive' approach resulting in accidents.

These issues are discussed in Chapter 3 with proposed guidelines presented for Industry consideration.

2.3.6 FAA Regulatory Training Review & Gap Analysis

2.3.6.1 FAA Training Regulations

The FAA has stipulated that Flight Crew require training (67) and that spaceflight participants require 'training' (66).

Training (based on standard Training Needs Analysis [TNA] approaches) should be detailed in more depth within the FAA guidelines and particularly so for SFPs due to their inexperience. Flight Crews will no doubt have been recruited from the military (fast jet pilots) and so will be more used to g-forces and emergency procedures. It is acknowledged that training must be tailored per vehicle type but there are general training needs irrespective of type.

Flight Crew Training Requirements

The FAA-AST splits the definition of flight crew and RLV pilot to state that the *pilot is on-board and who has the ability to exercise flight control authority over a launch or re-entry vehicle* as opposed to a flight crew member as *someone who is on-board and performs activities directly relating to the launch, re-entry or operation*. It is surmised that the FAA-AST are covering the possibility of a cabin crew member in addition to the pilots which seems reasonable. In terms of training however the requirements are more specific for a pilot in that;

> *"The pilot of an RLV that will operate in the National Airspace System (NAS) should possess an FAA pilot certificate, and should hold ratings to operate one or more aircraft with similar characteristics for as many phases of the mission as practicable"*

'Aircraft with similar characteristics' could be construed to be too generic because how many aircraft have rockets and also a glide to land characteristic? Also the operation will probably be carried out in a cleared (NOTAM) zone and although RLVs/SoAs will operate in the NAS it is within a completely different scenario. Yes the pilots should hold a current pilot certificate **and** they should have flown aircraft with medium to high 'g-forces' (more specifically and as an initial starting point, fast jet pilots are more suitable as they will have been trained to cope with high stress situations and cope with high 'g' should a non-nominal situation occur). Once the business is mature and safety has been demonstrated then the 'g-force' aspect could be relaxed to allow airline pilots to participate who may not have had fast jet experience.

Additional requirements for the flight crew which in this case may also include cabin crew:

> *"Each member of an RLV flight crew should be trained to operate the vehicle so that it will not harm the public"*

Here once again the FAA-AST focus on the public and this probably relates to flight safety systems and abort scenarios. However in addition there should be a requirement to be trained for on-board situations that have nothing to do with the public i.e. a SFP who may be either extremely sick or apoplectic, or someone who has had a heart attack and is dying.

Finally the following requirements concerning training equipment are stipulated:

> *"The RLV operator should verify through test, analysis, inspection, or demonstration that any flight crew-training device used to meet the training program requirements realistically represents the vehicle's configuration and mission*
>
> *RLV flight crew training should include nominal and non-nominal flight conditions. The non-nominal situations should include i) abort scenarios, ii) emergency operations, and iii) procedures that direct the vehicle away from the public in the event of a flight crew egress during flight"*

The Flight Crew training guidelines do not specifically state that Centrifuges should be used; instead they state that a 'training device' should be used that realistically represents the vehicle's configuration and mission. Arguably even a Centrifuge cannot accurately represent these (for instance if Virgin Galactic wish to provide Centrifuge training to their Crews in the 'NASTAR' facility, this is a generic device and may not be representable). They may also have a 'simulator' that represents the configuration and mission but this will have Fidelity and Capability issues and therefore could present hazards in its own right i.e. training the Flight Crew to experience something that is not real or representative.

Spaceflight Participant Training Requirements

The FAA-AST stipulates that SFP training is as follows:

> *"The RLV operator should provide safety training to each space flight participant prior to flight on how to respond to any credible emergency situations, which may include but are not limited to cabin depressurization, fire, smoke, and emergency egress"*

As a minimum, this is reasonable in terms of safety. However, other more likely situations will occur due to the medium to high 'g-forces' that the SFPs will encounter and it is these frequent issues that will lead to severe illness or even death (due heart attack or other people landing on each other and being crushed and unable to move during 're-entry'). There should be various levels of training ranging from awareness to experiential to emergency training. The SFPs will be interacting with the flight crew during the training (as well as the flight) and so this will aid in the 'teamwork' required for a successful flight.

Papers on Spaceflight Training

The author presented a co-authored paper at the 3rd International Association for the Advancement of Space Safety (IAASS) [70] including discussions on training and in particular the centrifuge device as key safety mitigation. The paper highlighted that first one must understand the accident sequence to understand the hazards and therefore what controls are required; in this instance a hazard of 'Excessive g-force to passengers' leading to a 'musculoskeletal' accident (G-Induced Loss of Consciousness [G-LOC]) resulting in black-out and death – here the safety mitigation (controls) suggested included:

- Design – Seats that move to assist with increase in g-force (both Gx and Gz orientation)
- Procedures – more benign profile (climb and apogee)
- Procedures – rigorous medical criteria
- Training – centrifuge experiences including the anti-g straining manoeuvre technique

2.3.7 Training Review Conclusions

The FAA has once again adopted the 'flexible' approach for the flight crew/pilots and also has not imposed specific training requirements for the spaceflight participants. The flight crew are required to undertake training in a suitable 'device' and SFPs are to be given a briefing. The main areas of concern are as follows:

- Flight Crew Training – As part of the User Requirements, the training devices for Crew should stipulate the use of centrifuges as well as simulators and that these should be as representative as possible in the following areas:
  - Fidelity; meaning the training devices' accuracy and 'trueness' in representing the flight conditions i.e. the visual system in a simulator provides real-world and high definition cues for the crew and SFPs. Also if 'flying' at Mach 3 in a vertical climb then the flight instruments represent this accurately.
  - Capability; meaning the ability of the training devices to perform the same as the platforms(s) in terms of flight profile i.e. capable of representing g-forces (in a centrifuge) and 'high-key' descent and approach path (high angle approach path during the glide to land phase)
  - Concurrency; meaning the training devices' equipment configuration in respect to the platform(s) i.e. instrumentation, seats, cabin windows (both in the centrifuge and simulator for instance)
- Participants Training – Basic pre-flight briefing on emergency aspects only. As

> the SFP is more 'engaged' in the flight that normal airline passengers, arguably they should have access to the same training devices as the Flight Crew and have a more defined schedule derived from (as with the crew) a formal Training Needs Analysis (TNA).

It is concluded that the FAA-AST should be more proactive and prescriptive in terms of SFP safety. Platform-specific TNA should be undertaken but the FAA should be able to provide a generic TNA model as a starting position for operators.

These issues are discussed in Chapter 3 with proposed guidelines presented for Industry consideration.

2.3.8 Review of Initial EASA Standpoint

2.3.8.1 Certification 'v' Licensing

EASA has stated their intent to undertake a different approach to personal and commercial spaceflight than that of the FAA-AST (as detailed in Section 2.3). The FAA-AST are following Licensing Rules for Launches based on the National Administration Legislation and are not requiring the applicants to certify their space vehicles per Federal Aviation Regulations.

EASA may follow known certification standards because of the definition in their position paper [76] for the activity which is based on the European Space Agency (ESA) definition[19]:

> *Suborbital flights [performed] by privately funded and/or privately operated vehicles*

EASA have added the following to the definition in their paper concerning the integration of suborbital flights into the EASA regulatory system [76]:

'*But limited to winged aircraft, including rocket-powered aeroplanes, and excluding rockets'*

They have further refined the term suborbital flights with 'Re-entry Launch Vehicles' (the FAA term) to Suborbital Aircraft (SoA). Arguably the main reasons for this is that the industry is immature (from a technical standpoint) and that the European Airspace is busy (from an operating perspective i.e. in America there are more remote locations to operate from). Thus, EASA will only consider 'aircraft'-based vehicles and will not consider vertical rockets i.e. the spacecraft must have wings. Furthermore the vehicle must be able to fly to the upper limits of the atmosphere (which can also be deemed the lower levels of space). This is a crucial operating boundary statement by EASA because they only have remit to certify an aircraft-based vehicle and therefore cannot certify the 'space' part of the profile; this important exclusion will be discussed further in 2.3.9.

There is a clear distinction between the FAA Licensing (whereby the Operator bears the full responsibility of its operations) versus the EASA certification approach (whereby the certifying authority takes a part of the responsibility).

The EASA approach identified in the paper would be a pragmatic one in which a SoA would be certified under existing (and equivalent) airworthiness codes for a Type Certificate (TC) or Restricted Type Certificate (RTC) as a basic starting point and then adapt it and complement it with Special

[19] Galvez A. and Naja G., on *Space Tourism*, in ESA bulletin 135-August 2008

Conditions (SC). An SC may be required when there are inadequate or missing standards as necessary to address:

- *Unusual features*
- *Unusual operations*
- *Features for which experience in service on similar design has shown that an unsafe condition may develop*

In terms of SoA the operating environment is clearly not normal for standard aviation vehicles and so the vehicle's ability to withstand excessive g-forces and microgravity conditions will require SCs. Additionally EASA is not normally presented with Rocket Propulsion Systems within an aircraft and so these in particular will have SCs applied.

The EASA paper then provides guidance on Technical Issues that would have to be addressed in addition to the §23.1309 criteria due to the specific characteristics and operations of SoA. The guidance included requirements for the following systems/issues whereby SCs may be required:

- *Environmental Control & Life Support System*
- *Smoke detection and fire suppression*
- *Personnel and cargo accommodation*
- *Emergency evacuation*
- *Emergency equipment*
- *On-board recorders*
- *Rocket Boosters/Engines*
- *Attitude/Reaction Control Systems*
- *Propellants*
- *Zero gravity operations*
- *Environmental Requirements*
- *Crew/SFP qualification & training*
- *Verification programme*

These systems will provide challenges for the designer and operator and they will have to work closely with the agency in meeting the requirements.

2.3.8.2 Equivalent Level of Safety

As part of the certification process EASA will determine an Equivalent Level of Safety (ELOS) that can be applied to SoA. This Thesis aims to provide assistance in this area in the provision of a Policy (and associated guidelines). In the update to the EASA position paper [76] EASA discusses the possibility of applying the current §23.1309 criteria [87] to SoA; this along with the results of this Thesis (as appropriate) will form the basis of a Policy and Guidance Material for Suborbital Airplanes (3.2).

2.3.9 Review of Suborbital 'Space Segment' Safety

EASA's boundary of their certification '*competence*' is up to the edge of space and is therefore limited to the air domain (and to aircraft rather than vertical rockets). This means that in Europe there is no one body (authority) that is regulating the 'space segment'. Even though this may only be for 3 to 5 minutes it is the phase of the flight whereby the SoA and its occupants are subjected to microgravity conditions and therefore additional safety mitigation is required. Although EASA and the FAA-AST have suggested technical considerations for the designer and operator to consider for the space segment of the flight to achieve their certification or launch license the actual requirements governing the use of the 'space' and explicit safety requirements are not regulated (within Europe).

Within the FAA-AST their remit for commercial spaceflight operations covers both orbital and suborbital and therefore for the suborbital designers and operators it is implicit that they are to meet the 'space' segment requirements. Within Europe however we will first have to understand the general principles of Space Law and Air Law in order to determine whether any demarcation is applicable or whether a 'transit' segment can be legally bound and agreed.

2.3.9.1 Space Law

The following table from the International Space University (ISU) paper on suborbital transport [77] Table 10 represents a summary of the principles of space law with the addition of observations made during recent space conferences:

Principle	Information	Comments
Legal basis	*Outer Space Treaty Ac, 1967. Applicable to space objects*	Suborbital flights will not reach outer space (although this will be argued as to the boundary)
Definition of space object	*Includes component parts of a space object, as well as its launch vehicle (Art. 2, Liability Convention, 1972)*	The space object (RLV/SoA) will enter the space segment
Fundamental principles	*Freedom of access implies the right of innocent passage to enter and exit space, though some States oppose this notion (COPUOS, 2005)* *Exploration and use of outer space for the benefit and in the interest of all countries* *No international regulatory standards*	As there is free access to space above the national airspace then States can arguably enter and re-enter as they see fit so long as they do not enter a neighbouring State unless they have pre-arranged agreements. Current Orbital re-entries do sometimes stray over other States without prior notice and this can be seen as a security breach. Current views (2nd IAA conference) are that suborbital should be considered within the Space Law domain and therefore go for licensing (over complex and expensive certification routes) and '*there are no rules on safety, standards or certification and no case law to interpret vague terms'*
Responsibility and liability	*States are responsible for national space activities and liable for damage caused by space objects under their jurisdiction.* *Private entities are subject to authorization and supervision of the State (Liability Convention, 1972)*	In this instance the US (FAA-AST) are mandating a launch and re-entry license within their own national space activity i.e. the intent is that the launch, re-entry and landing will take place within its own national boundaries (notwithstanding non-nominal trajectory issues).
Landing rights	*In case of unintended landing, the landing state must ensure protection and return of astronauts and space objects back to their national territory (Rescue Agreement, 1968)*	Not applicable to suborbital flights. The Space Shuttle has Transatlantic Abort Landing Agreements with Spain and France for instance
Liability Regimes – Damage caused by collisions	*Treated under OST, Article II* *Unlimited fault-based liability for collisions with other space objects* *Unlimited absolute liability for collisions with aircraft in flight* *No claims*	
Liability Regimes – Damage caused to 3rd parties on the Earth's surface	*Treated under Liability Convention, Article II*	
	Applicable for liability of the launching State The term "launching State" means: (i) a State which launches or procures the launching of a space object; (ii) a State from whose territory or facility a space object is launched (Article I) *Unlimited liability and absolute liability: no need for fault*	

Principle	Information	Comments
	No liability if: a launching state establishes that the damage as resulted from gross negligence or from an act or omission with intent on the part of the claimant state (Article VI) *Low history of third party damage claims* *Not applicable to nationals of the launching state or foreign national participants. (Article VII)*	
Liability Regimes – Damage caused to passengers	*Treated under Liability Convention, Article III*	
	Liability for damage sustained to passengers while inside the space object is not covered *Only if caused by another space object* *Unlimited fault-based liability (Article III)* *Not applicable to nationals of the launching state or foreign national participants (Article VII)*	The FAA-AST have stipulated 'liability cross-waivers' for crew and passengers (SFPs) i.e. they are to sign an 'informed consent' that they know the risks. The issues to be discussed are whether they will stand up in court and also as to the limit of the liability

Table 10: General principles of Space Law – adapted from ISU paper

2.3.9.2 Air Law:

As per Space Law above the following table presents a summary of the principles of air law;

Principle	Information	Comments
Legal basis	*Chicago Convention, 1944. Applying only to civil aircraft*	Applies to SoA/RLV
Definition of aircraft	*Any machine that can derive support in the atmosphere from the reactions of the air other than the reactions of the air against the Earth's surface (Annex 7, Chicago Convention, 1944)*	Hence EASA aims to certify only aircraft-based vehicles (SoA). The FAA-AST have used the term RLV and this applies to both aircraft-based and vertical rocket-based models so this aspect is different in the US
Fundamental principles	*Supreme and exclusive sovereignty of States in the airspace above their territory. Right of innocent passage applies to civil non-scheduled flights only. States may require such flights to land International Air Services Transit Agreement (IASTA, 1944) extends innocent passage to scheduled flights International Air Transport Agreement (IATA, 1944) Allows aircraft to embark and disembark passengers Bilateral negotiations for countries that have not ratified the IASTA or IATA International Standards and Recommended Practices applicable to all States*	These bilateral and multilateral traffic rights are based on intergovernmental air service agreements. ICAO believes that suborbital flight can be accommodated within the existing air law domain (a functionalist approach)
Responsibility and liability	*Contractual liability for damage to passengers and cargo owners (Warsaw Convention, 1929. Montreal Convention, 1999). Non-contractual third party liability on the ground (Rome Convention, 1952)*	
Landing rights	*n/a*	Covered in fundamental principles
Liability Regimes – Damage caused by collisions	*No direct provisions for collision of aircrafts with other aircrafts* *Likely to be based on fault under national law*	
Liability Regimes – Damage caused to 3rd parties on the Earth's surface	*Treated under the Rome Convention 1952 & Protocol 1978*	
	Applicable to liability caused by foreign aircraft to third parties on the ground *Limited liability depending on size of vehicle* *Unlimited liability for damage caused by deliberate act, omission with intent, or unlawful flight* *Strict liability standard* *No compensation if damage is not a direct consequence or results from fact of passage of the aircraft* *Low history of third party damage claims*	

Principle	Information	Comments
	National law will apply if damage is caused by a national aircraft	
Liability Regimes – Damage caused to passengers	*Treated under the Warsaw System & Montreal Convention*	
	Limited liability (low levels) *Based on fault and reversed burden of proof* *Unlimited Liability for wilful misconduct and absence of ticket* *Not liable if: all necessary measures were taken to avoid damage, or if damage is caused by negligence of the Plaintiff* *Elimination of liability ceilings* *A two-tier liability system*	

Table 11: General principles of Air Law – adapted from ISU paper

2.3.10 Space Law Conclusions

The 'space segment' phase of a suborbital flight is a contentious issue that is yet to be resolved. Within Europe it is clear that EASA is competent to certify vehicles within the Air Law domain yet are not competent within the Space Law domain. The question is 'Who is competent to provide regulatory oversight of the space segment for suborbital operations'? Is the ICAO competent or should this fall to a body such as the United Nations Committee on the Peaceful Uses of Outer Space (UN COPUOS)?

The ISU paper suggests that ICAO believes suborbital flight can be accommodated within the air law domain (a functional approach). Additionally the ISU paper suggests that the current space law is inadequate for commercial suborbital flights as the Outer Space Treaty concerns orbital aspects in the main. In terms of liability the paper states that:

> *"Operators and manufacturers will have to ensure that the appropriate levels of safety and reliability are met to prevent liability claims in excess of the capacity to handle them"*

Here the ISU are suggesting that the hazard and safety risk analysis should demonstrate that the system is safe; to do this properly the author of this thesis contends that a designer and operator would have to employ a safety case methodology and also provide evidence that their risks are reduced to 'so far as is reasonably practicable' (possibly using the ALARP methodology). The current FAA-AST guidelines are inadequate in that they do not explicitly detail that such rigour is required in the system safety analysis or operator safety risk management.

Interestingly in the space 'v' air law argument the common viewpoint of the industry is arguing for a space law approach to be more flexible with emphasis on a licensing approach under State responsibility. It is recognized that this approach (including the infamous 'waivers') should be implemented to allow the industry to grow with the eventual harmonization towards a more formal certification approach based on existing frameworks and filling in the gaps where applicable.

It is concluded that the argument of space law versus air law is far from over and as the suborbital industry fore-runners are currently in the initial test-phase of their development, that an answer to the debate is required as a matter of priority. This could include an initial agreement for invoking Space Law initially until the industry is more mature; this would require special agreements/considerations concerning suborbital specific issues as the main aspects of the Outer Space Treaty would not apply. Then a harmonized approach could be implemented based on the Air Law under ICAO authority in

which vehicles can be certified. These issues should be discussed at the IAASS Suborbital Space Safety Technical Committee (SSS TC) as a matter of urgency; here the SSS TC will be able to call upon the community to derive the way forward and implement this within the IAASS-ISSB Space Safety Standards Manual as 'good practice' and thereby use this as a 'lobbying' medium to the community and authorities.

Recommendation: It is recommended that the IAASS SSS TC review and resolve the issue of Space Law versus air Law; this recommendation is taken forward to section 6.4.

2.3.11 Review of Other Relevant Space Standards

This section aims to review other relevant space standards such as the European Co-Operation for Space Standardization (ECSS) and the IAASS-ISSB Space Safety Standards Manual.

2.3.11.1 European Co-operation for Space Standardization

The ECSS document set is vast and the review will focus on the main safety documentation and their relevance to the suborbital domain. The standards are produced as a co-operative effort between the European Space Agency (ESA), national space agencies and European Industry associations. The scope of the documents covers:

> *"the safety programme and the safety technical requirements aiming to protect flight and ground personnel, the launch vehicle, associated payloads, ground support equipment, the general public, public and private property, the space system and associated segments and the environment from hazards associated with European space systems"*

Space Product Assurance – Safety

The standard [79] is generally good and indeed is based on best practice. Section 5.0 (Safety Programme) is particularly good and can be used for suborbital designers. Section 6.0 (Safety Engineering) is also good and in particular details hazard detection – signalling and 'safing'. The term 'safing' appears a lot and as it is not defined[20] it can be assumed that it means to make safe i.e. a safing function (or system) could be a shielding from radiation or an emergency oxygen system and a 'safing procedure' could be the operation and use of such a system. The standard does specify safety of human spaceflight missions and has the following standards that must be met:

- *A mission abort capability shall be provided*
- *Safing and safe heaven functions shall be provided*
- *Escape and rescue functions shall be provided*
- *The capability to reconfigure the system to restore the functional capability of safety critical functions in case of failures or accidents shall be provided*
- *The capability to monitor, detect and assess hazards and effects of slow insidious events with hazardous consequences shall be detailed according to project constraints and mission objectives*
- *The space system shall provide an on-board medical facility and the capability for handling a permanently impaired or deceased crewmember (clearly this can be tailored for suborbital in that basic medical equipment could be carried).*

[20] Although not defined in the ECSS document the term 'safing' is defined in Table 1based on the ISSB Space Safety Standards Manual definition

The severity classification guidelines are not quite standard and have catastrophic as '*loss of life, life-threatening or permanently disabling injury or occupational illness*.' Arguably this is more applicable to the Critical/Hazardous severity because infers that one crewmember's death is catastrophic and clearly this is not the case; the loss of the 'Total System' (the ISS) and those on board would be catastrophic.

Section 6.6 also details operational safety band this also includes command and control from mission control i.e. not the crewmembers on-board and also includes ground operations

Section 7.0 details safety analysis requirements and techniques and is based on best practice.

Section 8.0 details safety verification aspects and once again is based on best practice.

The Appendices cover 'informative' and 'normative' guidelines which also appear useful.

Overall this ECSS is a good document to begin a suborbital safety management system but fails to be prescriptive in its actual safety criteria (surely ESA knows what criteria is to applied for products integrating with the ISS or going aboard Space Shuttles or Space Launchers). Also it fails to join up the design hazard analysis with operator safety risk management and therefore the total system risk or risk per accident type would not be known; once again disparate safety analysis would result from using the standard.

Space Product Assurance – Software Product Assurance

The standard **[**80**]** provides typical software safety best practice requirements including specifying software product assurance programme planning and detailing the handling of critical software. The remainder is based on best practice.

Appendix D [normative] (Tailoring of this Standard based on software criticality) is particularly good because it provides software criticality categories. Although they do not correlate to DO-178B or DO-254 (for the hardware/firmware) it does refer to its own system in relation to catastrophic, critical, major and minor severities:

Category	Definition
A	Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in: → Catastrophic consequences
B	Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in: → Critical consequences
C	Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in: → Major consequences
D	Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in: → Minor or Negligible consequences

Figure 38: ECSS Software Criticality Categories

2.3.11.2 IAASS-ISSB Space Safety Standard

The ISSB Space Safety Standards Manual [16] was briefly discussed in 2.1.2 and the purpose of this section is to put the review into perspective and to recommend a way forward. The standard is aimed at the Commercial Manned Spacecraft domain(s) and attempts to cover the suborbital domain as well as the orbital domain; it is considered that this was premature and as with the FAA-AST the standard is trying to cover too much in the same dialogue. The standard should be split into orbital and suborbital Chapters and where there is clear overlap then one chapter could refer to the other one. The technical chapters are good but should cover aspects such as software & computing systems (hardware/firmware) safety. The document states of its requirements as:

> *"The requirements in this document have been established on the basis of the safety experience accumulated in manned spaceflight to date. By demonstrating design compliance with these requirements, the commercial manned spaceflight operator will show to have taken into due consideration past experiences and best practices for the sake of making his spacecraft design and operations safe"*

The purpose of the manual and its associated Board (ISSB) is to provide flight safety certification services to the emerging commercial manned space industry and this is commendable. The manual should be updated (it was produced in 2006) and also aim to provide more rationalized guidance and best practice in terms of emerging knowledge over the past five years i.e. proposing a Class I aerospace medical for flight crew (instead of the FAA-AST Class I) and also to derive a harmonised approach to the licensing 'versus' certification approaches currently being debated. These are recommendations for the IAASS Suborbital Space Safety Technical Committee (which the author 'Chairs') – see 6.4 for the IAASS SSS TC recommendations.

2.3.11.3 Review of NASA/ESA Human Rating Requirements

Although mainly concerning orbital vehicles and operations Human Rating Requirements are suggested as possible alternatives to standard certification requirements. Indeed a paper at the 2nd IAA conference [78] proposes that these will be acceptable for commercial human rated space systems.

Human Rating Requirements were first derived in NASA whereby their definition stated that;

> *"a human-rated system is one that accommodates human needs, effectively utilizes human capabilities, controls hazards and manages safety risk associated with human spaceflight, and provides to the maximum extent practical, the capability to safely recover the crew from hazardous situations"*

ESA have also produced updated Human Rating Requirements and these are based on NASA's, the ECSS documents, ESA involvement in the ISS and from Lessons Learnt from the Challenger and Columbia disasters. Here ESA's definition is more focused on the safety technical requirements for human rating systems and state that they;

> *"are intended to protect the public, the ground and flight personnel, the space system, any interfacing system, public and private property and the environment from hazards associated with flight operations, and with ground operations with flight personnel on-board the system"*

They have also identified an explicit catastrophic safety target for orbital operations (Requirement 104.1) as *not exceeding $1x10^{-3}$ per mission* though they maintain that probabilistic risk assessment studies will still be the preferred method for crewed vehicles.

This section is included as an alternative route to certification and this type of approach may be suitable for commercial spaceflight operations in the US in the first instance and then, in the absence of EASA certification requirements, the ESA Human Rating Requirements could be tailored to the suborbital domain.

2.3.12 ISO 14620 Space Systems

Space Systems are also covered at International level with the ISO 14620 series. The series covers Space Systems Safety Requirements and is split into three parts: Part 1 covers System Safety Requirements; Part 2 covers Launch Site Operations; Part 3 covers Flight Safety Systems.

These standards are relatively high-level and although aimed at operators (such as a Launch site operator) they are also aimed at National Authorities i.e. *the quantitative safety objectives of hazardous systems with catastrophic or critical hazard related to a launch site should be established by the national responsible authority of the launch site country or by its authorized operators*[21]. Thus the standards do not provide the safety objectives or targets. This is disappointing and leaves the standards to lower level national authorities. In particular they should have provided guidance on the Expected number of Casualties (E_C) as opposed to leaving that aspect up to NASA; what about other national spacecraft launches? These standards are aimed at orbital spaceflight and so arguably as there are no specific safety objectives or targets then little can be extracted from them that the other lower-level standards have.

2.3.13 Review of Industry Safety Culture

The existing space safety culture has been criticised over the years as a result of the Space Shuttle accidents and as a result the space community has endeavoured to improve its safety management efforts. The author has witnessed the 'continuous improvements' by the likes of NASA from presentations at the IAASS conferences; there they have depicted an impression of a more cohesive approach i.e. 'Design' and 'HMI' teams working together and in a different session, 'Design' and 'Safety' working together. It was interesting to note the lack of total system safety approach i.e. Design **and** HMI **and** Safety **and** Operations; it is the author's view that due they will get to this 'generative' culture in the future because of the cancellation of Space Shuttle and NASA working new programs with commercial companies such as Space-X, Boeing and Armadillo Aerospace.

The fledgling suborbital industry has not yet taken flight but arguably the companies and authorities should be advocating and engendering a safety culture from the beginning. The review of FAA-AST safety-related guidelines in 2.3 highlighted a weakness in that the focus is on Launch Licensing (per the existing orbital safety methodology) and '*protecting the public'* (mainly 3rd parties on the ground but also other aircraft in the air). So for orbital companies such as Space-X they will just follow the 'normative' NASA-style approach. The author argues that for suborbital safety (and orbital) the companies involved are smaller in comparison to the NASA organisation and therefore should be able to establish a safety culture. However there is no mention of explicit safety management activities other than specific design features of the vehicles; clearly this is part of the overall safety effort but it is the view of the author that these small companies are designers and manufactures who are attempting to get a vehicle licensed under experimental terms with the aim of then obtaining Launch

[21] ISO 14620-2, Space Systems Safety Requirements, Part 2 – Launch Site Operations, page 8

Licenses for operations (with suitable waivers because the vehicles are not certified by the FAA). Taking Virgin Galactic or XCOR as an example they then aim to meet the FAA-AST regulations and guidelines by having a safety official (because it says so) and implementing an SSPP. Armadillo Aerospace for instance are an extremely small team of designers who are progressing very well and could actually beat these other bigger companies to flying a suborbital flight (it is a vertical take-off and landing craft with a much simpler design). They will at some point have to follow the FAA-AST licensing process and guidelines and appoint a safety official and have an SSPP; once again, in the opinion of the author, this will be an afterthought.

In Europe however, companies realise that they will have to follow an EASA-based regulatory approach and this requires companies not only to have a certifiable vehicle for airworthiness but to have an SMS approach and also obtain an AOC (for SoA). Herein lays the difference to the FAA-AST 'Experimental Licensing, Launch Licensing and waiver' approach – the early recognition that a Safety Management System is an essential component of the certification and operations. This will ensure that a safety culture is embedded not only throughout the company personnel but in the design of the vehicle due to the well-understood and best practice approach required of certification specifications i.e. systems engineering and systems safety management.

There is a great opportunity for a European company to have safety management as the differentiator in their approach to say that of Virgin Galactic, XCOR and Armadillo Aerospace. The *SATURN SAFETY MODEL* at section 3.4 provides a proposed method of a contiguous safety approach from designer to operator thereby requiring a joint approach in the safety effort. By implementing this model and approach a safety culture can be established right from the outset and this may prove crucial in terms of business success as a result of safety success.

2.3.14 Validation & Verification Summary for Suborbital Aircraft

In light of no new methodologies or rationalised approaches provided by the FAA-AST guidelines this section provides further thought on the V&V process in terms of issues presented by the suborbital industry.

Validation and Verification will be even more important in the nascent suborbital industry because unlike the aviation industry with millions of hours of history to call upon and with aircraft components tested until destruction or to meet specific requirements, the suborbital designers will have very little evidence to work from and thus are presented with extremely difficult challenges. In particular the novel designs constitute composite materials and the main issue and heart of the vehicles – the Rocket Propulsion System. The RPS may be 'off-the-shelf' systems or developed from new such as Virgin Galactic's hybrid rocket motor with rubber and nitrous oxide; here it will be extremely difficult to meet requirements.

What tools and techniques will be required to help demonstrate that the system has met requirements? Section 2.2.16 provided thoughts on future V&V processes stating that there were '*challenges in methods to deal with verification using low design data-intensity, to enhance the scope of functional verification with the development of integrated functional mock-up and techniques for the integrated product and process verification*'. Prospective designers will be engaged with Certification and Verification Engineers in providing design evidence through Computer Aided Design models, wind-tunnel models and even prototypes (of the RPS and of the vehicle as a separate entity). In most cases these two systems will be developed separately and then brought together for final assembly and integrated testing. Here is the challenge for the fledgling designers and the V&V will be essential in

detailing that requirements have been met; if this part of the analysis is not robust then the industry may get into difficulties before it has even left the ground.

2.3.15 Personal Spaceflight Review Conclusions

The Personal Spaceflight review has highlighted many areas of concern which stem from a clear lack of understanding the principles of Safety Management and in particular of the approach to take and how to use applicable criteria. The FAA are leading the way and do not want to stifle the new ventures by imposing too strict a criteria. However, the author considers the FAA is being too liberal in its use of the 'flexible' approach.

In regards to Safety Management there is a distinct lack of safety criteria and a lack of understanding of what constitute an 'Accident Sequence' and therefore what is required in terms of mitigation (controls). The FAA have not acknowledged there will be different RLVs with different flight/launch/land profiles and the 'Report to Congress' [81] have simply cited in their corroboration of the FAA documents that it is too early in the development to worry about whether Vertical and Horizontal craft should be considered separately.

The FAA Medical criterion is not sufficiently robust. It is concluded that the FAA have provided criteria that is not sufficiently robust and that having too flexible an approach may be detrimental in that some operators may follow the 'unrestrictive' approach resulting in accidents.

The FAA Training requirements are not sufficiently robust (in particular for participants).It is concluded that the FAA-AST should be more proactive and prescriptive in terms of SFP safety. Platform-specific Training Needs Analysis (TNA) should be undertaken but the FAA should be able to provide a generic TNA model as a starting position for Operators.

The FAA Launch Licensing approach to the airworthiness and hence certification of the prospective spacecraft would not be acceptable in Europe. For operations in America, the FAA clearly wants to let the nascent Industry grow by not requiring certification; in particular for the early experimental Licensing phase. Here the designers would be applying for an experimental permit to fly and would not be able to fly passengers. Following successful experimental flights the Operator would then have to apply for an Operator's Launch License.

EASA are adopting a pragmatic approach and one that is willing to certify aeroplane-based spacecraft (SoAs) under the existing regulatory framework with special conditions (SC) as appropriate. Within this framework, safety criterion is an essential component and the Equivalent Level of Safety for the SoA needs to be robust and defendable. The extant §23.1309 catastrophic failure condition criterion (in the order of $1x10^{-7}$ or $1x10^{-8}$ per flight hour) will be different to that proposed by the FAA-AST criterion (1E-6 per mission). Due to these differences in approaches it is clear that more specific and rationalised guidelines are required.

2.3.16 Current 'State' To 'Future State' Statement

The above conclusion highlighted that the current 'state' of the Personal Spaceflight Industry is immature both in commercialisation and in terms of Safety Management. There are many gaps in the current SMS guidelines for Design Organisations and Operators and these will become problematic in demonstrating that a Re-Launch Vehicle or Suborbital Aircraft is acceptably safe. The review conducted within Chapter 2 has highlighted these 'gaps' not only in terms of the fledgling industry's guidelines but also in the generic guidelines applicable to the aviation industry. To move forward to a 'future state', clearer guidelines are essential and Chapter 3 looks at innovative methods to fill the gaps.

CHAPTER THREE – Influence of Safety Management in Spaceflight

3. INTRODUCTION

The purpose of this Chapter is to ascertain whether the research has been able to influence Safety Management within the industry by three distinctly separate approaches; by practical application, by assisting in developing policies and by identifying new methodologies that could be applied to the industry (and possibly beyond). The aim is also to continue with the gap analysis undertaken in Chapter Two (Industry's 'current position') and determine whether a 'future state' can be proposed. The analysis of the review will be discussed concentrating on the three aspects:

- Section 3.1 – Setting up a new Suborbital Space Safety Technical Committee (SSS TC) in order to influence the community
- Section 3.2 – Providing assistance in determining Policy for Suborbital Aircraft (SoA) under EASA remit.
- Section 3.4 – Providing an Exemplar Safety Model appropriate for Commercial Spaceflight that can also set the standards for the aerospace sector and arguably other sectors with complex systems used by operators.

3.1. SUBORBITAL SPACE SAFETY TECHNICAL COMMITTEE

The author has been a member of the International Association for the Advancement of Space Safety (IAASS) since 2006 and has presented papers on safety management aspects at the IAASS conferences (see Appendix 8 through 12). With the emergence of the suborbital industry there is growing awareness (and concern) within the IAASS regarding the new field. To that end and after being on the Suborbital Space Safety Panel at the 4th IAASS conference in May 2010, the author proposed to the President of the IAASS that a new Suborbital Space Safety Technical Committee (SSS TC) should be formed to address the emerging issues. On the 31st March 2011 the proposal was agreed and the author was invited to Chair the SSS TC, form a suitable committee, provide suitable topics and ensure any overlap with other TCs was suitably managed. This has been progressed and an Explanatory Note was submitted to the IAASS (see APPENDIX 13 - Safety Suborbital Space Safety Technical Committee 'Explanatory Note').

3.1.1 Technical Committee Initial Task

The author (as the Chair of the SSS TC) formed the committee from the regulators, industry forerunners, and specialists with suitable skills. A kick-off teleconference was held on 1st July 2011 to welcome the members and to outline the strategy and to update the members from the presentations of the 2nd IAA [54]. The author then presented the initial task for the committee which was for each member to summarise the current status within their area concerning suborbital space flight; this would then be presented as a paper (and poster presentation) at the 5th IAASS conference in October 2011. The author also explained that the SSS TC would be further split into sub-committees with the following domains:

- Regulatory/licensing; this would cover the current and difficult topic of Licensing 'versus' Certification and look towards a possible harmonized approach. Additionally this group would cover Spaceports and different criteria for vertical RLVs and aircraft-based SoAs.
- Technical (System Safety); this would cover the technical issues concerning the vehicle(s)
- Operational Aspects' this would cover training, medical and flight standards

Note: At the time of submission the TC has been split into the three sub-committees and the following topics have been selected for each to discuss and present at the 5th IAASS conference:

- Regulatory Group – 'Regulating the Space Sector'
- Technical Group – 'Survivability/Recoverability of Suborbital Aircraft'
- Operations Group – 'Spaceport Safety Considerations'

3.1.2 Technical Committee Further Work from Thesis Recommendations

It is considered that any specific and relevant recommendations from the Thesis is presented as agenda items for the IAASS SSS TC; the recommendations will be discussed at workshops or for internal papers and as appropriate to update the IAASS ISSB Space Safety Standards manual [89].

3.2. SUBORBITAL AIRCRAFT – EASA POLICY

Based on the results of the gap analysis (current state) of the FAA Rules & Guidance, it is necessary to try and move to a 'future state' that has a robust safety argument as its provenance. The FAA-AST will need to update and improve upon their guidance in the near future as 'operators' will soon be unveiling SoA /Reusable Launch Vehicles (RLV) in order to start their Test & Evaluation phase. Once this phase is complete the real operators have also stated their intent to operate from Europe and other parts of the world (Virgin Galactic proposing to operate from Sweden, Scotland and the Middle East, and XCOR proposing to operate from Spain, Germany and Korea).

Within Europe, EASA need to develop its own safety governing Rules & Guidance such that future SoA Designers/Manufacturers, Operators and current Spaceports can work within the same [robust and rationalised] Safety Management System. This Chapter focuses on providing rationale for an EASA Policy as part of their Regulatory Framework. Thereafter operators would have to follow the standard certification aspects in accordance with the SoA Policy.

It is recognised that Europe does not have rules or guidelines that are specific to SoA operations within the EASA framework. To enable some form of rules and guidelines to be implemented within Europe, EASA was tasked to provide a Preliminary Regulatory Impact Assessment (Pre-RIA) in order to determine whether EASA needed to take any action regarding SoA and also to what level of action. The author was tasked to assist EASA in this preparatory step. The projected roadmap to the EASA SoA Pre-RIA includes the following:

- Pre-RIA; this activity involved working with the EASA SoA team to derive the rationale for proposing an EASA Regulatory activity. This covered identifying the following;
  - *The market*
  - *The main hazards/risks (high level risks based on known and generic profiles)*
  - *The baseline assessment in terms of*
  - *Safety risks and issues*
  - *Environmental risks and issues*
  - *Economic risks and issues*
  - *Societal risks and issues*
  - *Regulatory Co-Ordination and Harmonisation*
- Assessment of Options
  - In this instance the option chosen was to implement an SoA Policy

The next phase will begin when and if the European Commission approves the SoA rulemaking task; the next steps will include:

- *Terms of Reference*
- *Full RIA; this expands on the Pre-RIA in order to justify fully the impact of the activity*
- *SoA Policy (the option chosen as part of the Pre-RIA process); this includes the requirements and the guidelines for SoA operations*
- *Notice of Proposed Amendment (NPA) detailing;*
- *Explanatory Note*
- *The SoA Policy*
- *The full RIA*
- *Public Workshop; it is necessary to engage the 'public' which essentially means the interested industry organisations and can also include the view of the general public.*

3.2.1 EASA SoA Policy – Model

To assist in the development of a robust EASA SoA Policy 'future state' the following Model has been constructed in order to demonstrate the robustness and applicability of the Policy. The model is based on the Goal Structuring Notation (GSN) not only because it provides a visual argument as to the claim that the SoA Policy is effective but that a goal-based regulatory approach can be a pragmatic way of introducing the new Policy. Indeed J Penny et.al from the UK CAA and co-authors from the consultancy 'Adelard' discussed such an approach in their paper [90];

> *"Goal-based regulation" does not specify the means of achieving compliance but sets goals that allow alternative ways of achieving compliance, e.g. "People shall be prevented from falling over the edge of the cliff". In "prescriptive regulation" the specific means of achieving compliance is mandated, e.g. "You shall install a 1 meter high rail at the edge of the cliff". There is an increasing tendency to adopt a goal-based approach to safety regulation, and there are good technical and commercial reasons for believing this approach is preferable to more prescriptive regulation. It is however important to address the practical problems associated with goal-based regulation in order for it to be applied effectively*.

Another driver for adopting goal-based regulation, from a legal viewpoint, is that overly-restrictive regulation may be viewed as a barrier to open markets. Various international agreements, EC Directives and Regulations are intended to promote open markets and equivalent safety across nations. Whilst it is necessary to prescribe interoperability requirements and minimum levels of safety, prescription in other areas would defeat the aim of facilitating open markets and competition. Finally, from a commercial viewpoint, prescriptive regulations could affect the cost and technical quality of available solutions provided by commercial suppliers.

The Top-Level is produced below in Figure 39 and the full SoA Policy GSN including the argument and evidence is contained at APPENDIX 5 - Suborbital Aircraft Policy – Goal Structuring Notation.

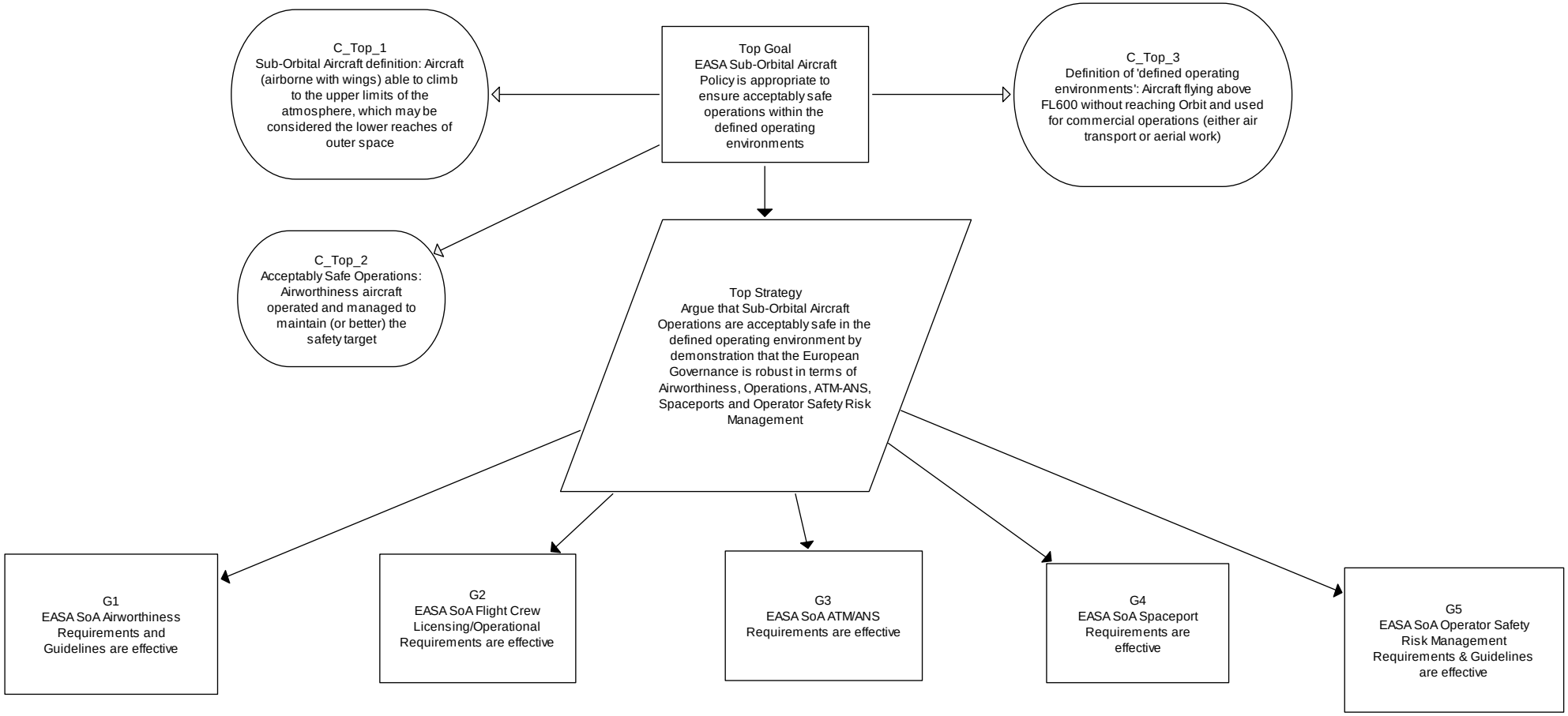


Figure 39: EASA Suborbital Aircraft Policy Goal Structuring Notation

3.2.2 EASA SoA Policy - Safety Case Framework

The EASA SoA Policy is summarised below and the full Policy Goal Structuring Notation is at APPENDIX 5 - Suborbital Aircraft Policy – Goal Structuring Notation. At the time of thesis submission the European Commission were debating as to whether the SoA Policy task should proceed following the Pre-Regulatory Assessment and therefore the task is not complete.

Top Goal: The EASA SoA Policy is appropriate to ensure safe operations within the Air Domain

The Context of which the 'Top Goal' is defined as follows:

- Context 1 [C_Top_1]: Definition of SoA - Aircraft (airborne with wings) able to climb to the upper limits of the atmosphere, which may be considered the lower reaches of outer space
- C_Top_2: Definition of Acceptably Safe - Airworthiness aircraft operated and managed to maintain (or better) the safety target
- C_Top_3: Definition of Air Domain – Aircraft flying above FL600 without reaching orbit and used for commercial operations

The **Top Goal** is supported by a Strategy (**Top Strategy**) which demonstrates that the EASA SoA Policy is robust to ensure safe Suborbital commercial operations. This Top Strategy is supported by 5 strands of the argument; EASA SoA Airworthiness Requirements are effective - **Goal (G1)**, EASA SoA Flight Crew Licensing/Operational Requirements are effective - (**G2**), EASA SoA ATM/ANS requirements are effective - (**G3**), EASA SoA Spaceport Requirements are effective (**G4**) and EASA SoA Operator Safety Risk Management Requirements & Guidelines are effective (**G5**):

(G1): EASA SoA Airworthiness Requirements are effective:

The recent, rapid and successful developments in the domain of commercial spaceflights have highlighted the need to develop corresponding regulations in order to protect the flight crew and passengers on board a SoA and also to ensure the risks to the non-involved people on the ground or in the air are appropriately mitigated.

The EC legislator gave responsibility of aviation safety to EASA, including airworthiness, air operations and flight crew licensing. In relation to commercial spaceflight, EASA's remit focuses on aircraft, the definition of which excludes rockets and capsules. EASA's scope in regulating commercial spaceflight also accords with European Space Agency's (ESA) definition of space tourism as '*suborbital flights [performed] by privately funded and/or privately operated vehicles'*[22] but (in EASA's viewpoint [76]) *limited to winged aircraft, including rocket-powered aeroplanes, and excluding rockets*. Thus EASA's remit is focused on 'Suborbital Aircraft' as:

> *"This term encompasses both the operational pattern (suborbital, therefore requiring less speed/energy to climb and be spent on return) and the type of vehicle, namely an aeroplane (airborne with wings) able to climb up to the upper limits of the atmosphere, which may be also considered as the lower limit of outer space"*

This means that EASA intend to govern any commercial suborbital operations within Europe in accordance with their existing regulatory framework and hence the **argumen**t (to support the goal G1)

[22] Galvez A. and Naja G., on *Space Tourism*, in ESA bulletin 135-August 2008

is based on the current EASA processes and procedures concerned with regulating aeroplanes, supplemented with Special Conditions and supported by relevant existing FAA-AST regulations and guidelines.

G1 is supported by two sub-goals:

(a) (G1.1); Applicable Basic Requirements are effective for SoA Operations The evidence to support this goal is that EASA has the authority of the European Commission and from the Law (the Basic Regulation) by which Member States have transferred their competence to undertake airworthiness certification. To achieve this EASA issues Type Certificates based on an aircraft meeting airworthiness codes in the form of Certification Specifications (and in particular to SoA, CS-23) and acceptable means of compliance as appropriate.

(b) (G1.2); Additional Special Conditions and requirements are identified and are effective for SoA operations. The argument that Special Conditions (SCs) are identified is that EASA has considered the systems of the SoA in the suborbital operating environment and have derived additional (special) certification requirements.

The evidence provided in the Appendix details the specific extant basic regulations (such as EASA 831, 8411 and 1450 for ECLSS) and identifies additional SCs and guidelines for system requirements (such as initial considerations for ECLSS), human factors considerations (FAA-F460.15) and non-air breathing propulsion systems to name a few. The evidence refers to the FAA-AST regulatory and guideline aspects where these were considered relevant (such as FAA-AST 460-11 for ECLSS). There was however FAA-AST aspects that were not considered appropriate for EASA Policy such as the safety objectives requirements. In this instance EASA plans to base the final criterion on a rationalised approach aligned from CS-23 but modified and complemented for SoA requirements.

Note: in this perspective EASA has suspended the task whilst the EC make their final decision on the rulemaking priorities. However based on the author's analysis the recommended approach should be to adopt a 'Safety Target' approach (top-down) but to also have implicit 'safety objective' requirements for failure conditions (bottom-up). The rationale is that the RPS is the driving failure condition and arguably will take up a lot of the Safety Target's risk budget (typically at best $1x10^{-4}$ per mission). With a catastrophic Safety Target in the order of $1x10^{-4}$ to $1x10^{-5}$ per flight hour, then it is clear that the modelling of the RPS will rely heavily on the exposure factor being added in at the system analysis level and also this will drive designers to incorporate safety features as mitigation in order to try and achieve the overall system safety target. By having failure condition safety objectives set as additional requirements this will enable designers to optimise the existing technologies with well-defined and low probability values with the more novel design features with un-proven reliability data hence providing a challenge to the systems analyst. A Safety Target of $1x10^{-5}$ per flight hour means a derived system level failure condition safety objective of $1x10^{-8}$ per flight hour. As mentioned this should be achievable for most systems however the RPS analysis (with exposure factors and safety features) may achieve $1x10^{-6}$ per flight hour; this equates to 90% of the Risk Budget and therefore by summing the other system's safety objectives the overall target will be 'bust' i.e. it will not meet the requirements. A more realistic catastrophic safety target would be **$1x10^{-4}$ per flight hour** because then the designer will have a realistic chance of at least getting to within one order of magnitude of the target (due to the RPS) but hopefully the designers may be able to achieve the target. In the case where the target is not met (but within one order of magnitude) then the argument should provide operator mitigation such as:

- Additional safety features in the event of a fire/explosion

- Operator Limitations: Only initiate the RPS in a designated remote corridor
- Operator Procedures: Abort procedures, etc.
- Operator Training: Training for non-nominal events

Further rationale for setting the safety target at $1x10^{-4}$ pfh is that this is the order of magnitude that industry experts have derived; these views are from the IAASS-ISSB Space Safety Manual and designer views (such as Reaction Engine's abort methodology for Skylon's certification path) and the target is close to the FAA-AST guidelines. Additionally to put the target into perspective this is 100 times safer than the Space Shuttle and equally 100 times less safe than commercial aircraft with millions of hours of service history to validate the origins of safety objectives. This appears a reasonable baseline for the start of the development phase. Arguably over time and with more than 1000 safe flights then a probability function may start to be derived that is more aligned with a CS-23 Class III aircraft.

Evidence (G1): The evidence is incomplete at the time of submission.

(G2): EASA SoA Flight Crew Licensing/Operational Requirements are effective:

The argument for G2 is that EASA has existing Flight Crew Licensing (FCL) requirements and these will form the basis of the SoA FCL requirements. The argument is then to provide additional identified requirements towards the SoA FCL requirements; flight crew are deemed 1st party personnel for legal and safety classification reasons. In addition to flight crew EASA is required to provide requirements for space flight participants (SFPs); these are deemed to be 2nd party personnel (see definitions Table 1 for 1st and 2nd party definitions). In this area of FCL and SFP requirements the approach taken by the FAA-AST is considered not as stringent as it should be and hence the differences in requirements are stated.

G2 is supported by two sub-goals:

(a) (G2.1); FCL and SFP requirements are identified and specific to SoA operations; 1st party requirements (flight crew) are considered more stringent than those of transport aircraft flight crew due to the exacting environmental aspects that they will be exposed to and hence the criterion should be set high – in particular for the early phases of the nascent industry. Hence EASA consideration is for a licensed air transport or commercial rated pilot; in addition consideration could be for a SoA specific rating of flight test pilot standard and/or military fast jet pilot standard (in particular for the test phases and early commercial flights). The medical standards are for a Class I Aerospace Medical Certificate (as opposed to a Class II required by the FAA-AAST). The rationale is backed up by aerospace medical practitioners and in particular in a paper [67] on suborbital medical issues. In terms of training, the FAA-AST guidance [71] is considered acceptable for EASA requirements: however in addition in regards to training requirements EASA considers that centrifuge training is mandatory for flight crew whom should be trained to cope with Gz and Gx (this is not stated within the FAA-AST guidelines); also that hypobaric training (within an altitude chamber) is also mandatory such that flight crew can recognize the signs and symptoms of decompression so that emergency procedures can be quickly implemented (donning an oxygen mask and selecting 100% pressure breathing as an example). In terms of SFPs EASA concurs with the standard medical checks performed by the individual's General Practitioner and also the operator's flight surgeon prior to training and prior to flight. However EASA's approach is that SFPs require training as safety mitigation so that they do not become a flight safety concern during the flight and therefore affect the flight crew's ability to maintain control of the vehicle. Therefore in addition to the FAA-AST 'safety briefing' training [66] EASA plans to mandate centrifuge training and simulator training as a minimum. In particular the

simulator training and safety briefs will cover normal procedures and also focus on non-nominal drills; these considerations for emergency drills are detailed in the GSN at the Appendix but include pressurisation failures, fire, loss of control (as per Scaled Composite's SS1 flight) and crash landing/emergency egress.

(b) (G2.2); Operational requirements and guidelines are identified and specific to SoA operations; this goal requires further work as it is not complete. Operational requirements will consider single-pilot operations for example as there is a single-piloted craft being developed in America (XCOR's Lynx SoA) and they stated their intent to fly within Europe. Additional considerations will concern remote telemetry and control; safety critical systems such as the RPS should have relevant parameters that are monitored by telemetry and by cockpit instruments (such as pressures, temperatures etc.) such that malfunction procedures or reconfiguration can be employed to result in a safe configuration (safing) before reaching a catastrophic condition. In this instance the FAA-AST requirements should be acceptable for EASA operations (FAA-AST 417.307). Furthermore EASA will only certify SoA (as opposed to vehicles with expendable rocket boosters) and therefore will adopt Special Conditions for 'Thrust Termination Systems' as opposed to Flight Termination Systems or Flight Safety Systems (though the later could be included as this can also mean the pilot as part of the flight safety system). In this respect the FAA-AST requirements (431.35(5) will need modifying to meet EASA requirements so as to protect the occupants of the SoA as well as the 'public'.

Evidence (G2): The evidence is incomplete at the time of submission.

(G3): EASA SoA ATM/ANS requirements are effective:

The argument is that EASA has an existing and effective Air Traffic Management (ATM)/Air Navigation System (ANS) that is underpinned by aviation law in the European Union and these will form the baseline for SoA policy. The argument is then to provide additional identified requirements that would accommodate SoA in the existing framework. The Goal is supported by two sub-goals:

(a) (G3.1); Existing ATM/ANS Requirements and guidelines are effective. These are well established and based on Regulation (EC) 1108/2009[23]. This goal requires more substantiation.

(b) (G3.2); Additional SoA ATM/ANS Requirements and guidelines are identified and are effective; The integration of SoA into the current ATM/ANS system will require additional requirements and guidelines to assure the safety of the SoA, other aircraft and the uninvolved public (3rd parties). The main areas in terms of the following:

- Flight Planning:
  - Issue a NOTAM of the intended suborbital flight. The NOTAM will provide sufficient mitigation to exclude other air vehicles. This must be for a 'corridor' of specified altitude, length and width. Additionally under §437.57 'Operating Area Containment';
    - this mainly concerns protecting the public on the ground and that the planned trajectory (orbital connotations) and non-nominal trajectory should remain within the containment area
  - Ensure standard integration and separation with aviation traffic when not in the 'corridor'.
  - Ensure the maximum altitude of the NOTAM is no greater than 150km (above this altitude the NOTAM is no longer valid and the Operator must

[23] http://www.skybrary.aero/bookshelf/books/940.pdf

seek orbital collision avoidance analysis)

- The Spaceport authority should also ensure that the NOTAM area has minimal (or none) populated areas i.e. over the desert, inhabitable mountains or over the sea
- The Spaceport authority should provide 'windows of opportunity' for SoA/RLV Operators whereby the air traffic is 'light' within or near the corridor; this can reduce the exposure of other air traffic thereby reducing the exposure to a mid-air collision

- Flight Rules:
  - Separation; normal rules apply for the SoA within standard controlled and uncontrolled airspace when not in the 'space flight corridor'. Additionally §437.71 – Flight Rules apply;
    - (b)(1) *Follow flight rules that ensures compliance with §437.57 (above)*
    - (d) *A permittee may not operate a reusable suborbital rocket in areas designated in a Notice to Airmen (NOTAM) unless authorized by ATC*
  - VFR-IFR; depending on design the operator must be certified for either VFR only or VFR-IFR if the appropriate equipment is within the design of the vehicle.
  - Communications; standard communications apply when within controlled and uncontrolled airspace which accords with §437.69.

Evidence (G3): The evidence is incomplete at the time of submission.

(G4): EASA SoA Spaceport Requirements (*additional requirements to aerodromes*) are effective:

The argument is that Spaceport Requirements are effective and this is partly substantiated because current aerodromes are required to be certified and the FAA has CFR Part 139 [99] which is appropriate. Additionally to the requirements of CFR Part 139, the FAA introduced AC 150/5200-37 [26] which details SMS guidance for Airport Operators. The argument is then to provide additional identified requirements that would accommodate SoA in the existing aerodrome framework to enable it to become a Spaceport. New-build Spaceports should be able to be designed to the SoA Policy requirements based on the existing aerodrome framework as well as additional requirements. G4 is supported by the following:

(a) (G4.1); SoA Spaceport Requirements & Guidelines are identified and are effective; the existing requirements of FAA-AST CFR 420 [96] detail the requirements for Spaceports effectively including the explicit safety objective in terms of risk to the 'public' per mission ($E_c \leq 30 \times 10^{-6}$). Additionally the explosive siting part, CFR 420 §420.63 to 69, covers the following very well;

- *An explosive site plan*
- *Safe storage of rocket propellants (RP) (assumes RP-1)*
- *Safe handling of rocket propellants*
- *Issues of Solid and Liquid propellants located at same spaceport*
- *Calculated minimum separation distance (of combined propellants)*
- *Intervening barriers*
- *Crowd (public) safety within the bounds of the spaceport – depends on*

the vehicle type and propellants used.

Additionally CFR 420 §420.71 concerns lightning protection at the launch site.

These CFR 420 requirements can be amplified with the FAA-AST Environmental guidelines [95] where safety aspects are relevant (such as airspace, health & safety, hazardous materials and hazard waste management and noise).

Evidence (G4): The evidence is incomplete at the time of submission.

(G5): EASA SoA Operator Safety Risk Management Requirements & Guidelines are effective:

This argument involves new approaches in which EASA intend to adopt a 'Total System' approach to include FCL, Operations and ATM/ANS as well as airworthiness. In terms of safe operations, although guidelines do exist for air operators, such as ARP 5150, it is considered that EASA provide specific guidelines for the nascent industry such that operators will be able to integrate their Safety Management System (and Operator Safety Risk Management) with the design organisation's system safety analysis for certification requirements. The rationale is that the 'Total System' is then managed effectively. This is considered achievable because the design organisations will be working extremely close with the operators and in some cases these may well be one in the same organisation. This then calls for a contiguous safety effort which will enhance the certification process. This may be even more important should a specific SoA design not meet challenging safety objectives or a safety target. The goal is supported by two sub-goals:

(a) (G5.1); Operator Safety Risk Management requirements are identified and effective for SoA operations; Here it is EASA's intent that operators are required to have a formal Safety Management System which incorporates a Hazard Management System. Operators should provide a Safety Management Plan which details the high level safety requirements and safety targets/safety objectives and these should then flow down as derived safety requirements to the design organisations (DO) system safety analysis; indeed the SMP will be the baseline from which the DO provides their System Safety Program Plan (SSPP). This document then details how the Operator's Safety Requirements will be met by the designed system. This way a contiguous safety effort can be achieved which provides safe assurance for the 'Total System'.

- Additionally operators are to obtain an Air Operating Certificate (AOC) per their aviation counterparts. This may have Special Conditions applied due to the novel environmental and operating conditions.

(b) (G5.2); Operator Safety Risk Management guidelines are identified and effective for SoA operations; There is a gap between the DO guidelines such as ARP 4754/4761, ECSS documents and Advisory Circulars such as AC437.55-1/ AC431-35-2A (for commercial spaceflight hazard analyses and system safety process – which is a mixed guidelines for DOs and operators for obtaining an experimental launch permit) and operator guidelines such as ARP 5150 (and AC120-92) and ECSS document with basic operator information. Therefore EASA will provide guidance for operators (this has not been completed as yet – it is intended that the supplemental considerations in section 3.3 is reviewed with the EASA SoA team and incorporate as guidance material as necessary).

Evidence (G5): The evidence is incomplete at the time of submission.

3.2.3 EASA SoA Policy – Conclusions

The EASA SoA Policy safety case presented is a Top-Level GSN and this has been developed for the thesis to show that the Policy meets the top goal (the full argument is presented at APPENDIX 5 - Suborbital Aircraft Policy – Goal Structuring Notation).

The GSN uses a goal-based approach because the aim was to set Policy i.e. standards, regulation and guidelines. The argument concludes that the Policy is robust within the existing EASA regulatory framework but that Special Conditions (SC) are required because of the novel designs and novel operating environment. The evidence is based on existing regulations and guidance with the addition of FAA-AST regulations and guidance. However it was found that some areas of the FAA-AST information was not appropriate for EASA regulatory and guideline purposes and therefore this was highlighted and additional standards proposed based on further evidence from industry experts, such as the Aerospace Medical Working Groups for determining appropriate flight crew standards.

Although the argument is robust for the defined operating environment (up to, but not including the 'space segment') the SoA clearly enters the space segment for nominally 3-5 minutes and therefore the safety of the SoA is not certified under EASA for that phase of the flight. This is a major safety issue and one that needs to be addressed within Europe; the FAA-AST does not define the limits of their jurisdiction and therefore do not have the issue. This is carried forward to the IAASS Suborbital Space Safety Technical Committee recommendation Chapter 6.4.

At this time (submission of the thesis) EASA have not yet continued with the Policy and are awaiting further approval from the European Commission. Therefore the SoA Policy is not fully substantiated, meaning that not all arguments and evidence has been completed and therefore validated by the EASA team. When the SoA Policy is endorsed by the EC it is recommended that the author continues the SoA Policy Regulatory safety case with the EASA team; this recommendation is carried forward to the general 'further work' Chapter 6.3.

Additionally, 'supplemental' or supporting analysis has been provided in the next section and is deliberately and explicitly detailed in depth such that EASA could determine whether to keep the Policy 'high-level' to provide flexibility or whether EASA wanted to be more explicit in their guidelines to assist Designers and operators.

3.3. **SUPPLEMENTAL GUIDELINES FOR CONSIDERATION**

As the EASA Policy is purposely high level, it was considered necessary to further analyse the aspects identified within Chapter 2 and in particular the gaps that were identified. The purpose of this section in addition to the EASA Policy is therefore to provide any rationale (that would otherwise not be prudent within a Policy document) and to be more explicit (as opposed to generalising a requirement or guideline).

3.3.1 Safety Objectives

It is important to establish safety criteria and in the early phases of development, testing and operation this may be difficult to achieve – especially covering different modes of spacecraft designs and profiles (aluminium-based 'v' composite and horizontal 'v' vertical take-off/landing etc.). However, a baseline must be established from which to work from. The FAA have implicitly determined that their risk acceptability criteria is related to individual hazards and that they will fall in the 'high' category (Hazard Risk Index 1-6 & 8) or the 'low' category (HRI 7 & 9-20). This approach may be satisfactory for hazard risk acceptability classification; however it does not allow for additional levels of accident risk acceptance and would hinder rather than assist in management ownership and decision-making. Furthermore how have they derived the numerical probabilities and does the criterion apply to all spacecraft? – as opposed to aviation air vehicles, suborbital spaceflight operators intend to have different profiles (horizontal 'v' vertical take-off/launch and landing) and hence will have different risks. So do we need to consider separate tables or have additional criteria within the same classification table? Also during these early stages how does the Industry set Safety Targets and hence derive Hazard Risk Budgets?

The review and gap analysis in 2.3.2 highlighted the following deficiencies:

- No Safety Target (and consequently no Hazard Risk Budget)
- Poor Safety Risk Acceptance Criteria
- Severity only to 3rd Party (the public and the public's property)
- No Accident List

The above highlights the deficiencies in the FAA-AST system that needs to be corrected in order to be acceptable within an EASA regulatory framework. The following sections supplement the EASA SoA Policy argument for SoA operations:

Accident (Loss) Safety Target

The FAA guidance [18] does not include a Safety Target or indeed a Hazard Risk Budget (seeing as the Risk Matrix is a hazard-based Matrix). A Safety Target is important as it reflects the Risk of the vehicle; in essence it is the cumulative probability of technical failures/faults i.e. of the failure condition probabilities. Within civilian aviation it is recognised that the safety target is 'loss of aircraft (and ergo loss of life) due to technical safety critical failures should be no greater than 1×10^{-7} (1 in 10 Million flights). This 'incredible' figure is due to the extensive testing and history in the aviation industry; this is based on the total Loss of aircraft probability of $1x10^{-6}$ per flying hour. For the immature suborbital spaceflight industry this probability will not apply due to unproven technologies flying in unproven and harsh environments. Therefore a realistic probability must be set. It is proposed that the Accident (Loss) Safety Target is $1x10^{-4}$ per flying hour for Loss of the SoA (the catastrophic A/B line for SoA). The rationale follows the '1309' philosophy that 10% of accidents are due to critical systems and with 100 'hazards', the single hazard (failure condition) budget is set at three orders of magnitude lower i.e. $1x10^{-7}$ per flying hour. The rationale is that the early stages of

development operational flights could be conducted with non-human payloads and flight crew (to gain experience). Then when sufficient hours are accumulated such as 1000 hours the safety target may be reviewed and arguably set at $1x10^{-5}$ per flying hour which is a preferred and more socially acceptable target i.e. only one order of magnitude less than current aviation. Initially the argument is that the nascent suborbital industry safety target is two orders of magnitude worse than aviation but over two orders of magnitude better than the Space Shuttle therefore this puts it into perspective for the public.

Although the Accident (Loss) Safety Target is a 'top-down' approach, it still accords with the bottom-up approach of using safety objectives for individual failure conditions (as described above for a Part 23 Class III aircraft). Therefore the current certification framework (for normal aircraft) applies to SoA. With the implementation of a top Safety Target, the DO Safety Manager will be able to work closely with the Operator's Safety Manager in order to:

- Comply fully with failure condition's safety objectives
- Partially comply with failure condition's safety objectives by being within one order of magnitude;
  - In this instance DOs should be able demonstrate that other critical systems have more than achieved their safety objective and therefore a trade-off in probabilities will ensure the design criteria are still met
- Not comply with failure condition's safety objectives by more than one order of magnitude;
  - Examples of this instance will be the SoA Rocket system whereby industry knowledge can at best provide a predictive occurrence rate of $1x10^{-4}$ or $1x10^{-5}$ per flying hour. In this instance the DO must discuss the following with the Operator in order to take further credit in the analysis

In this instance where catastrophic failure condition's safety objectives have not been met, per the §25.1309 guidelines [46] as detailed by the ARAC report:

An acceptable alternative method is to perform all of the following:
(1) Demonstrate that well proven methods for the design and construction of the systems in question have been utilized; and
(2) Determine the average probability per flight hour of each failure condition using structured methods, such as fault tree analysis, markov analysis, or dependency diagrams; and
*(3) Demonstrate that the **sum** of the Average Probabilities per Flight Hour of all Catastrophic Failure Conditions caused by systems is **extremely remote**.*

Here using the above guidelines a DO must engage with the operator and continue the analysis from the failure condition to a specific accident because then they will be able to apply the following operator-based procedures and limitations in order to further reduce the risk to the system.

- Operator Limitations – these should be agreed and adhered to in order to take appropriate credit;
  - Limit the area of operation to a restricted zone (limit to 3rd parties)
  - Limit the exposure time of the rocket i.e. it might be nice to fly higher to 150km, but actually by limiting the apogee to 110km, then further credit can be taken
  - No Limitations And Exceptions (regarding deferrable faults concerning the rocket)
- Operator Procedures – these can provide good mitigation on most aspects apart

from a rocket explosion, however notably the following may apply;
    - Flight Termination System (FTS)/Thrust Termination System (TTS) – this is a key procedural requirement to enable the pilot to abort the flight by shutting off the rocket should any anomalies be detected.
- Air/Ground Segment Operating Parameters Monitoring – safety critical systems such as the Rocket system should have relevant parameters that are monitored by telemetry and by cockpit instruments (such as pressures, temperatures etc.). This is such that malfunction procedures or reconfiguration can be employed to result in a safe configuration before reaching a catastrophic condition.
- Maintenance/Operator Procedures (Dormant Failures) – these can be specific to a system such as the Rocket whereby analysis identifies a switch that could potentially fail that requires checking before flight (or a switch that enables the mixing of the oxidizer for instance – better this results in a fire/explosion on the ground than a catastrophic explosion in flight)

Risk Acceptance Criteria

The FAA-AST guidance [18] Risk Acceptance is essentially either a pass of a fail in that there are two categories:

- *Category 1 – High (1-9); Elimination or mitigation actions must be taken to reduce the risk*
- *Category 2 – Low (10-20); Risk is acceptable*

This is unfortunately a step backwards in that the previous version included a 'Medium' risk category which allowed Operators the ability to manage risk and to accept those conditions which may not have met the criteria (such as rocket systems). This 'single' line is more akin to the criterion required of Design Organisations i.e. a failure condition's safety objectives.

The EASA Risk Acceptance Criteria should in the first instance set a safety target and supplement this with explicit safety objectives for certification using Table 17. Then the designers should work with the operators using the Risk Matrix in Table 19; this allows an element of risk acceptability whereas the FAA-AST system does not allow Operators to accept risk.

Accident Lists

The FAA guidance (2) does not include an Accident List as per normal aviation analysis; these are detailed in the ICAO SMSM [24]. The FAA-AST has not stipulated a total system 'accident list' because they have opted for a hazard risk management approach without rationale for safety targets or risk budget. This is because the failure condition approach is for Design Organisations (DO) and the FAA are currently dealing with DOs attempting to gain an 'Experimental Permit' to fly.

The proposed scheme utilises the accident risk management approach and aligns with aviation categorisation of 'accidents' (as detailed in Section 2.2.5.2). In general there are in the order of 10 accidents applicable to an aircraft and these can be assumed to be the same as on a spacecraft; following on from this, it can be assumed that there are 10 safety critical 'hazards' contributing to each accident, therefore an aircraft (spacecraft) could have 100 hazards. Each hazard would then be assigned a risk budget in order to meet the total system (accident) safety target. As EASA recognise the higher-level ICAO guidelines, the following generic aircraft (spacecraft) accidents are proposed based on the ICAO accident list; the list has been modified by rationalising those descriptions that could be a subset of another accident in order to provide clearer definitions and are presented in the AMC/Guidelines for EASA:

Accident No.	Accident Title	Accident Description	Notes/ Accidents Not Used (due subset of other SSE)
A1	CFIT	Controlled Flight Into Terrain – CFIT leading to loss of aircraft [assumes loss of all personnel on board]	
A2	MAC	Mid-Air Collision (MAC) leading to loss of aircraft [assumes loss of all personnel on board]	
A3	LOC-I	Loss of Control – In flight (LOC-I) leading to loss of aircraft [assumes loss of all personnel on board]	System/Component failure or malfunction – non-power-plant Note – this would lead to LOC so is not included
A4	LOC-G	Loss of Control – Ground (LOC-G) leading to loss of aircraft [assumes loss of all personnel on board]	
A5	Explosion	Explosion (Fuel Related) leading to loss of aircraft [assumes loss of all personnel on board]	
A6	Fire (flight)	Fire during flight* leading to loss of aircraft [assumes loss of all personnel on board]	*Flight considered from engines running to engine shutdown) – 'smoke' in itself will lead to incapacitation and/or loss of visibility in cockpit for example and therefore would lead to a different accident such as CFIT or LOC-I/G
A7	Fire (non-flight)	Fire on the ground not in flight, including post survivable crash and pre-engine start leading to loss of aircraft [assumes loss of all personnel on board]	
A8	Loss of Thrust	Loss of Thrust (system/component failure or malfunction – power-plant) leading to loss of aircraft [assumes loss of all personnel on board]	
A9	Structural Failure	Structural Failure leading to loss of aircraft [assumes loss of all personnel on board]	

Table 12: Proposed Exemplar Accident List

The accidents above assume loss of spacecraft and loss of life. A single death (of a passenger for instance) is considered an accident however this is classified as a 'Critical' severity (for 1st /2nd Parties).

Along with the Accident List, there is also a list for 'Serious Incidents'. These are also detailed as Safety Significant Events in ARP 5150 [75] and are defined in the ICAO Taxonomy [49]. The ICAO definition of a 'Serious Incident' is '*An incident involving circumstances indicating that an accident nearly occurred'*.

The severity Table 15 further below also includes Incidents (Serious, Major, Minor) and is relevant to the Safety Model. The list of Serious Incidents (SSEs) in the ICAO taxonomy is as follows; once again per the accidents, the list has been modified by rationalising those descriptions that could be a subset of another SSE in order to provide clearer definitions:

Accident No. (SSE)	Safety Significant Event Title	Safety Significant Event Description	Notes/ SSE Not used (due subset of other SSE)
SSE1	Near MAC	A near collision requiring an avoidance manoeuvre, or when an avoiding manoeuvre would have been appropriate to avoid a collision or an unsafe situation (near MAC)	
SSE 2	Near CFIT	Controlled flight into terrain (CFIT) only marginally avoided An aborted take-off on a closed or engaged runway, or a take-off from such runway with marginal separation from obstacle(s)	A landing or attempted landing on a closed or engaged runway Take-off or landing incidents, such as undershooting, overrunning or running off the side of runways
SSE 3	Fire/Smoke	All fires and smoke in the passenger compartment or in cargo compartments, or engine fires, even though such fires are extinguished with extinguishing agents	
SSE 4	Near LOC-I (System failures In-Flight)	Multiple malfunctions of one or more aircraft systems that seriously affect the operation of the aircraft	Failure of more than one system in a redundancy system which is mandatory for flight guidance and navigation
SSE 5	Crew Incapacitation	Any case of flight crew incapacitation in flight	
SSE 6	Emergency Oxygen Use	Any events which required the emergency use of oxygen by the flight crew	
SSE 7	Near Structural Failure	Aircraft structural failure or engine disintegration which is not classified as an accident	
SSE 8	Fuel Emergency	Any fuel state which would require the declaration of an emergency by the pilot	
SSE 9	Near LOC-I (performance)	Gross failure to achieve predicted performance during take-off or initial climb/rocket phase	
SSE 10	Near LOC-I (Ops)	Weather phenomena, operation outside the approved flight envelope or other occurrences which could have caused difficulties controlling the aircraft	'System failures' removed from this category as they are really covered by the description in SSE4

Table 13: Proposed Exemplar Serious Incident (Safety Significant Event) List

Inherent-based hazards (OHHA & OSHA as described in 2.2.4) should be linked to a relevant accident so that the event can be managed at the appropriate level i.e. explicitly managed and controlled below the hazard level or explicitly managed and controlled at the accident level (and beyond to the consequences – in order to reduce severity for instance). Chapter 2.2.5.2 discussed various inherent-based hazards leading to 'Inherent Accidents' and within the safety model these need to be explicitly detailed. These Inherent Accidents are more difficult to name and some guidance is available in the European Safety and Health at Work publications and medical definitions. An example is a slip-trip hazard leading to musculoskeletal accident and this can have varying severities such as minor injuries (Minor severity in Table 15 below) to individual death (Hazardous/Critical severity in Table 15 below). The following table presents the proposed Inherent Accident List necessary to undertake the joint DO-Operator safety analysis per the new safety model:

Inherent Accident No.	Inherent Accident Title	Inherent Accident Description	Notes
IA1	Musculoskeletal	An event whereby the body has suffered a muscle or skeletal-based trauma	
IA2	Cardiovascular	Where changes in cardiac rate and function could lead to a heart attack	
IA3	Neurovestibular	An event whereby the body has suffered from a conflict between visual, vestibular, and proprioceptive stimuli leading to dizziness, pallor, sweating, and severe nausea and vomiting	
IA4	Pulmonary Function	An event whereby the body has suffered from difficulty in breathing (includes asphyxiation and loss of oxygen due pressurisation issues)	Although this may lead to heart attack (IA2 above) it is distinct in its classification in particular to spaceflight and therefore warrants its own Accident classification
IA5	Burns	An event whereby the body has been affected by electrical, fluid or solid fires or energy transfer	
IA6	Aural	An event whereby excessive noise results in injury	
IA7	Ocular	An event whereby excessive light results in injury	

Table 14: Proposed Exemplar Inherent Accident List

These Inherent Accidents could all credibly lead to a hazardous severity with the consequence as death. They could also lead to Major (severe injuries) and Minor (slight injuries) or even Negligible (discomfort) events; all should be explicitly linked and managed because the flights may become not socially acceptable if people are vomiting every flight or are returning on every flight with Minor injuries through g-forces.

SoA Accident Severity Classification

The FAA guidance [18] interestingly applies severity to the hazard (actually hazard-accident cell that combines probability and severity in the Risk Matrix). The above citation from paragraph 5b of [18] focuses on effect to *the public* and to *property*. Also within the severity category table, Catastrophic is only '*death or serious injury to the public'* and the Critical category is '*major property damage to the public, major safety-critical system damage or reduced capability, significant reduction in safety margins, or significant increase in crew workload'*; it is considered that the FAA have based their criteria on the current NASA approach (as opposed to aviation best practice), which essentially looks at risk of launch and launch trajectory mishaps with the harm to the public and property being the focus. The proposed severity categories for the EASA approach consider the effect to people, the asset and the environment:

- 1st Parties – individuals directly involved in operating the spacecraft/suborbital aircraft
- 2nd Parties – individuals directly involved in supporting the spacecraft/suborbital aircraft (i.e. maintainers) and individuals participating in the flight who are not members of the flight crew (i.e. passengers)
- 3rd Parties – the uninvolved public
- Asset – Loss of, damage to and degradation of performance of the spacecraft
- Environment – damage to the environment (from explosions or rocket fuel leaks)

Description & Category	Actual or Potential Occurrence	Effect To People			Effect to Asset	Effect to Environment
		1st Parties	2nd Parties	3rd Parties		
Catastrophic	Accident	Multiple 1st Party deaths	Multiple 2nd Party deaths	Single 3rd Party death	Loss of spacecraft	Extreme widespread environmental damage
Hazardous	Serious Incident - Asset or Accident (people death/injury)	Single 1st Party death Physical distress or excessive workload impairs ability to perform tasks	Single 2nd Party death	Multiple Serious injuries 3rd Party (requires hospital treatment more than 2 days)	Severe damage to spacecraft Large reduction in Functional capabilities or safety margins	Severe environmental damage
Major	Major Incident	Multiple Serious injuries/ illnesses to 1st Parties (requires hospital treatment more than 2 days) Physical discomfort or a significant increase in workload	Multiple Serious injuries/ illnesses to 2nd Parties (requires hospital treatment more than 2 days) Physical discomfort	Single Serious injury to 3rd Party (requires hospital treatment more than 2 days)	Major damage to spacecraft Significant reduction in functional capabilities or safety margins	Major environmental damage
Minor	Minor Incident	Minor injuries/illnesses to 1st Parties (requires first aid and/or hospital treatment for less than 2 days) Slight increase in workload	Minor injuries/illnesses to 2nd Parties (requires first aid and/or hospital treatment for less than 2 days)	Minor injury to 3rd Parties (requires first aid and/or hospital treatment for less than 2 days)	Minor damage to spacecraft Slight reduction in functional capabilities or safety margins	Minor environmental damage
Negligible	Occurrence without safety effect	Inconvenience	Inconvenience (requires assistance and is reportable)	Single Minor injury to 3rd Party	Less than Minor damage	Less than minor environmental damage

Table 15: Proposed Severity Classification

The severity classifications in Table 15 also include the Part 23 definitions in terms of reduction in safety margin and increase pilot workload.

SoA Probability Classification

Table 16 reflects an ELOS of a Part 23 Class III aircraft however, due to the Special Conditions and using a Safety Target approach for SoA, the safety objective is set at $1x10^{-7}$ per flying hour for 'extremely improbable' catastrophic failures (as opposed to $1x10^{-8}$ per flying hour for Class III aircraft).

Likelihood	Quantitative Description	Qualitative Description
Frequent	$X > 10^{-2}$	Likely to occur one or more times in the life of the system
Probable	$10^{-2} > X > 10^{-3}$	Likely to occur several times in the life of the system
Occasional	$10^{-3} > X > 10^{-4}$	Likely to occur sometime in the life of the system
Remote	$10^{-4} > X > 10^{-5}$	Remote Likelihood of occurring in the life of the system
Extremely Remote	$10^{-5} > X > 10^{-6}$	Unlikely to occur in the life of the system
Improbable	$10^{-6} > X > 10^{-7}$	Extremely unlikely to occur in the life of the system
Extremely Improbable	$X < 10^{-7}$	So unlikely, it can be assumed occurrence may not be experienced in the life of the system

Table 16: EASA SoA Proposed Likelihood/Probability

Option 1: Safety Objectives Approach for Design Organisations

Option 1 is a safety objectives approach: The Safety Objectives Risk Matrix at Figure 40 reflects an Equivalent Level of Safety for a Part 23 Class III aircraft and has been extrapolated into a cohesive and logarithmic Risk Matrix. The DOs must adhere to the set criteria as per normal certification requirements for each severity of failure condition as defined in the Part 23 Functional Hazard Analysis. In terms of SoA there will also be Special Conditions to consider.

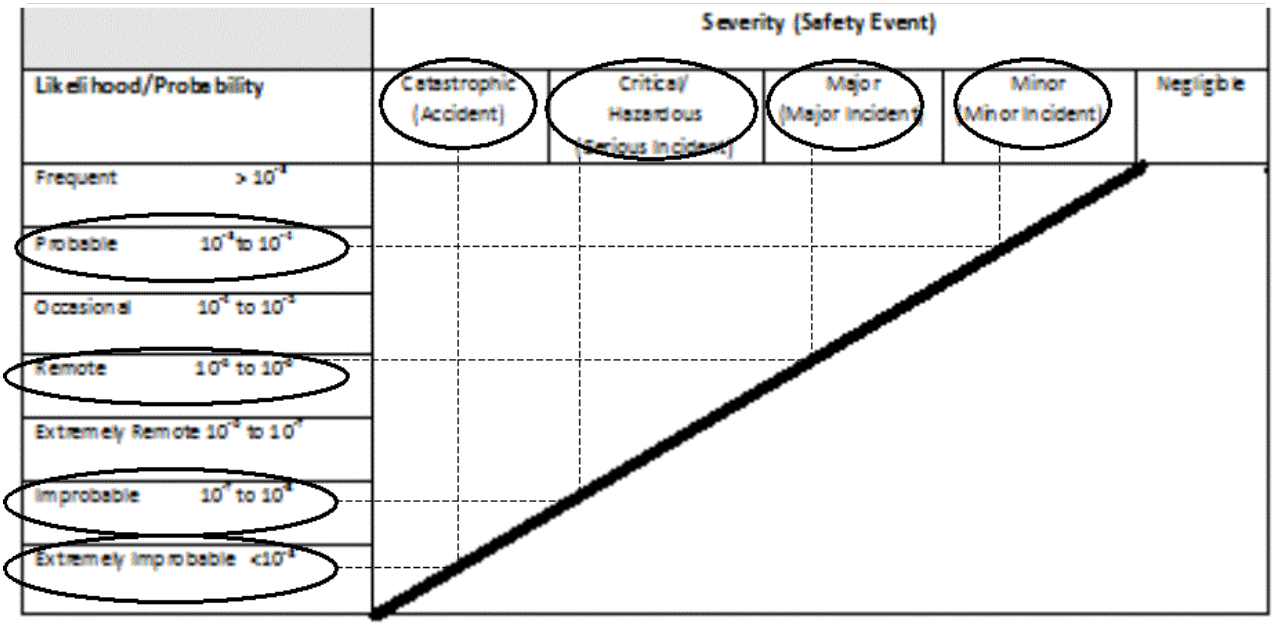


Figure 40: Standard Safety Objectives Approach for Design Organisation

The option 1 approach is what design organisations are used to however it is acknowledged that the nascent suborbital industry will have difficulty in meeting such rigorous safety objectives in particular for the RPS.

Option 2: Safety Target Approach for Design Organisations

Option 2 is a safety target approach: The Safety Target approach at Table 17 is calibrated for 100 hazards (per severity classification) such that the safety target of $1x0^{-4}$ per flying hour will not be exceeded so long as the number of failure conditions per cell multiplied by the numerical value in the cell does not exceed the value of 1000 (this is merely a value and not a hazard risk index). The table is

calibrated this way such that it is explicit to design analysts that the safety target must not be exceeded and that it allows for systems that will not meet a safety objective of $1x10^{-7}$ per flying hour such as the rocket propulsion system (RPS). In terms of systems like the RPS it will drive designers to achieve better than $1x10^{-4}$ per flying hour even if by just a slight margin. Should this not be achievable and a design has this one failure condition at the $1x10^{-4}$ per flying hour level then this means that the other 99 failure conditions must be below the $1x10^{-7}$ per flying hour threshold to achieve the overall target. In this instance due to the RPS, the designer would argue their case with the regulatory authorities that the safety target has been met due to the remaining 99 failure conditions being acceptable (less than the acceptable safety objective threshold of $1x10^{-7}$ per flying hour).

Note: By implementing a contiguous safety model approach (as per the *SATURN Safety Model*) then the design analysis will continue to the operator analysis. In cases where the design criterion has not been met then in **exceptional circumstances** the designer could argue the case by a combination of engineering judgment and operator judgment and using the continued accident sequence as evidence that the residual risk is acceptable; this must be within the 'tolerable' region within the operator's risk matrix.

The assumption for this method in the early phases of design analysis is that the top of the cell is taken as the probability value i.e. 'Improbable' equates to $1x10^{-6}$ per flying hour; the rationale is to be more conservative with the estimations. Clearly the designer may wish to use the mean value of the cell in order to take the average value of the cell i.e. 'improbable' could now equate to $5x10^{-7}$ per flying hour. As more analysis and evidence is gathered then the actual probability values can be taken and therefore the cumulative values (per severity classification) will be more representative.

In the exemplar table below it is only the yellow and amber (tolerable) values that are cumulatively summed i.e. the red is unacceptable and the green cells (acceptable) are not summed because the designer has met the implicit safety objectives and therefore their contribution to the safety target is already accounted for.

	Severity (Safety Event)				
Likelihood/Probability	Negligible	Minor (Minor Incident)	Major (Major Incident)	Hazardous (Serious Incident)	Catastrophic (Accident)
Frequent $> 10^{-2}$	**100**	**1000**	**1001**	**1001**	**1001**
Probable 10^{-2} to 10^{-3}	**10**	**100**	**1000**	**1001**	**1001**
Occasional 10^{-3} to 10^{-4}		**10**	**100**	**1000**	**1001**
Remote 10^{-4} to 10^{-5}			**10**	**100**	**1000**
Extremely Remote 10^{-5} to 10^{-6}				**10**	**100**
Improbable 10^{-6} to 10^{-7}					**10**
Extremely Improbable $<10^{-7}$					

Table 17: Proposed Designer's Safety Target (Failure Condition/Hazard) based Risk Matrix for Designers and calibrated for 100 hazards per severity. The number of hazards in the cell is multiplied by the numerical value in the cell and this along with the other tolerable cells shall not exceed 1000 when cumulatively summed

So to be explicit there are really three safety targets for designers:

(a) Catastrophic Safety Target – $1x10^{-4}$ per flying hour

(b) Hazardous Safety Target – $1x10^{-3}$ per flying hour

(c) Major Safety Target – $1x10^{-2}$ per flying hour

(d) Minor Safety Target – not set; best practice arguments apply

In terms of Negligible classifications these should also be managed but do not require a safety target as there should be no safety occurrence.

Further rationale is to link the design analysis with the operator safety risk management as detailed further below. The operator safety risk management uses the same probability and severity definitions and risk areas (the shape of the risk matrix) but their analysis is concerned with the **accident risk management**. This is achieved by managing the operating procedural controls, training controls and limitation controls higher up the accident sequence as described in section 3.4.

SoA Failure Condition Classifications and Probability Terms

(a) In assessing the acceptability of design, EASA recognised the need to establish rational probability values based on an Equivalent Level of Safety but mindful of the Special Conditions applicable to SoA.

- The classification of failure conditions should be conducted per best practice as defined in AC§23.1309 with the probability definitions per the guide in Table 17 above.

SoA Identification of Failure Conditions and Considerations assessing their effects

As detailed in Chapter 2.2.4 it is necessary to conduct an FHA at the beginning of a project. In this instance Design Organisations will conduct the FHA for their SoA and will develop their Functional Block Diagrams (FBD) down to System level in order to determine the relevant failure condition from which to base their design and system safety analysis. A 'partial' FHA is already contained within AC 23.1309 [87] and this was intended as guidelines for smaller, Part 23 aircraft design organisations that may not be used to standard requirements as per their Part 25 counterpart design organisations. Nevertheless the partial FHA can be considered as a useful starting point for a SoA (which is arguably a Part 23 type of vehicle). Prior to conducting an FHA from an SoA FBD, it was considered a useful exercise to develop the §23.1309 partial FHA and to include SoA specific failure conditions based on the author's knowledge of the various SoA designs and from the FAA-AST relevant guidelines and EASA paper [76]. In this instance to capture the SoA functions (and carrier aircraft as appropriate) two additional columns have been added to the FHA table to ascertain whether the failure conditions were applicable or not and to insert pertinent failure conditions for the SoA and carrier aircraft (integration thereof). The partial FHA is detailed at APPENDIX 6 - Exemplar Suborbital Aircraft (Partial) Functional Hazard Analysis – Failure Condition Level.

In addition to the 'partial FHA' detailed in (a) above, it is further considered that a generic (partial) aircraft-level FHA is necessary to derive safety requirements and safety objective criteria. Additionally this would have been conducted prior to a System level FHA as standard practice. An aircraft-level FHA is defined in ARP 4761 [85] as:

> *The aircraft level FHA is a high level, qualitative assessment of the basic functions of the aircraft as defined at the beginning of aircraft development. An aircraft level FHA should identify and classify the failure conditions associated with the aircraft level functions. However, if separate systems use similar architectures or identical complex components and introduce additional aircraft level failure conditions involving multiple functions then*

> *the FHA should be modified to identify and classify these new failure conditions. The classification of these failure conditions establishes the safety requirements that an aircraft must meet. The goal in conducting this FHA is to clearly identify each failure condition along with the rationale for its severity classification.*

A generic SoA Functional Block Diagram (FBD) has been constructed to provide an initial baseline for the FHA. The FBD has been derived by following standard aviation-based functions. These functions have then been broken down into separate functions which in turn break down to lower-level specific functions. The FBD is base-lined at a high level such that the initial platform level FHA can be conducted:

- To Aviate (fly)
  - To provide thrust
  - To provide control of the aircraft (in the air)
  - To provide control of the aircraft (on the ground)
  - To provide structural integrity
  - To provide visibility
- To Navigate
  - To provide awareness of aircraft state (in terms of attitude, altitude, heading and speed)
  - To provide aircraft current position and flight path data
- To Communicate
  - To provide external visual clues (meaning to communicate visually)
  - To provide external communications
  - To provide internal communications
  - To provide external data communications
- To Transport (including containment)
  - To provide habitable areas
  - To provide crew seats/restraint
  - To provide passenger seat/restraint
  - To provide normal ingress/egress
  - To provide emergency egress
  - To provide ability to contain aircraft fluid systems
  - To provide ability to contain aircraft equipment
  - To provide ability to release containment of fluids
  - To provide ability to air carriage (SoA transported by Carrier Aircraft)
- To Display aircraft conditions
  - To detect and warn of aircraft conditions
  - To manage equipment and systems operation

Figure 41 below details some of the identified functions and then further breaks them down to a level from which platform-level hazards may also be derived (Key (Platform) Hazards – see 3.4.4).

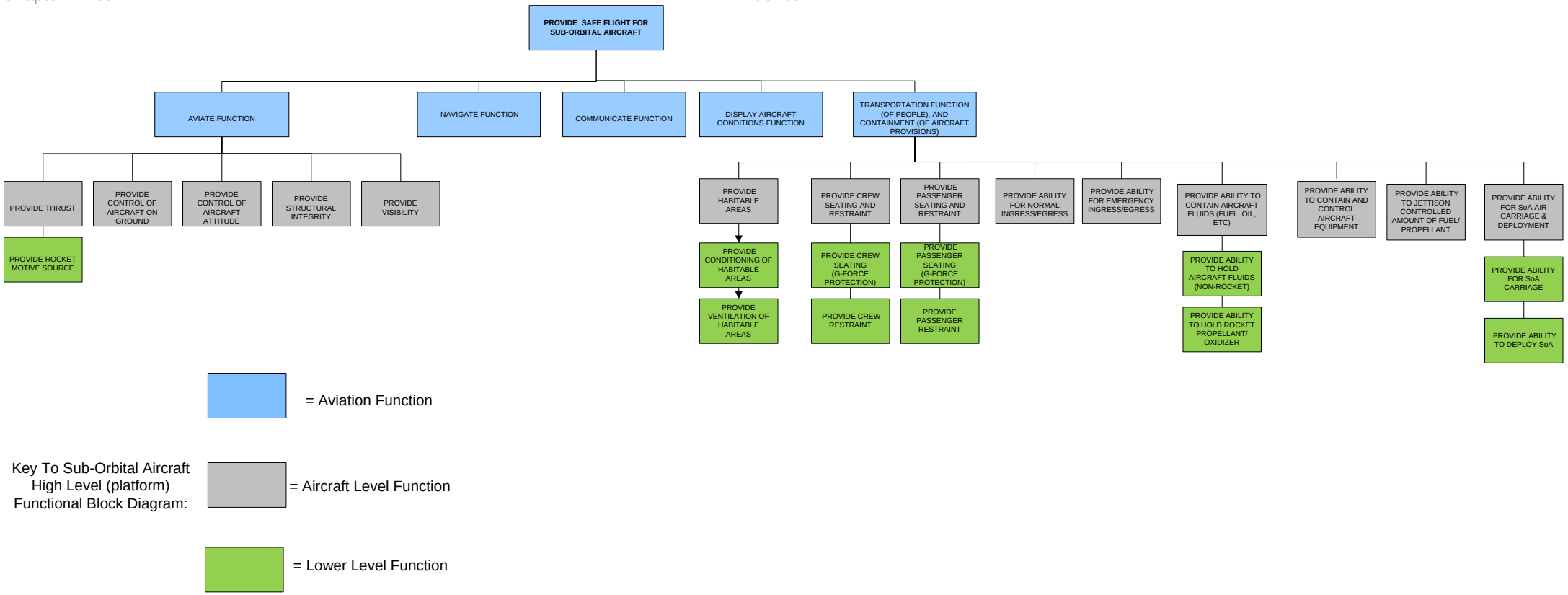


Figure 41: SoA Functional Block Diagram – Partial Top Level Shown As Example

(a) The aircraft level FHA inputs (from ARP 4761) are as follows:

- The list of top-level functions (from the FBD such as Lift, Thrust, etc.)
- The aircraft objectives and customer requirements (e.g. number of passengers, range, etc.)
- Initial design decisions (e.g. number of engines, conventional tail, etc.)

In terms of the generic (partial) FHA for SoA the second and third points above relate to individual projects however it will be assumed the SoA is a standard 'business-jet' like aircraft with aero-engines in addition to a rocket and that it will have a 'carrier' aircraft for an air-launch (a carrier aircraft is also chosen to include the 'integration' aspects). The SoA FHA is at APPENDIX 7 - Exemplar Suborbital Aircraft (Partial) Functional Hazard Analysis – Aircraft Level. The FHA was derived from the following sources:

- AC 23.1309
- EASA paper
- Authors knowledge and interpretation of systems

The FHA established whether the functional requirement was applicable to the SoA and/or the Carrier aircraft (integration aspects only as the aircraft will be certified in its own rights). The SoA aspects that were generic such as the provision of a 'flight control system for the pitch axis' were deemed 'applicable' and this judgment continued for the other identified requirements. Those aspects that were derived as SoA specific and of interest are included in the summary table below:

		Classification of Failure Condition				Comment	
Systems	**Function**	**Total Loss of Function (with warning)**	**Loss of Primary Means of Providing Function**	**Misleading and/or malfunction (without warning)**	**General Functional Failure (Loss or Incorrect)**		Comments and Applicability to **Suborbital Aircraft**
Systems	Reaction Control System	Hazardous	Hazardous	Catastrophic		Engineering Judgment - additional identified for Suborbital ops	RCS must be able to operate and not interfere with normal controls any stability augmentation system
Systems	Display of toxic gas levels	Catastrophic	Catastrophic	Catastrophic		Engineering Judgment - additional identified for Suborbital ops	closed loop system so need to ensure levels of CO2 are not high and incapacitate pilots
Power-plant (Excess Loads)	Rupture of pressurised components (oxidiser tank)				Hazardous		Catastrophic for SoA
Power-plant (Excess Loads)	Abnormal thrust vectors				Variable - engineering judgment required; Hazardous?	Causes by engine mount failures, inadvertent thrust reverser deployment, compressor surge, nozzle failures	Nozzle blockage/ asymmetric ablation
Power-plant (thrust)	Rocket Thrust Loss				Major to Hazardous	Engineering Judgment - additional identified for Suborbital ops;	In this instance, the SoA would abort the rocket phase and recover stability and then do a normal glide/approach

		Classification of Failure Condition				Comment	
Systems	**Function**	**Total Loss of Function (with warning)**	**Loss of Primary Means of Providing Function**	**Misleading and/or malfunction (without warning)**	**General Functional Failure (Loss or Incorrect)**		Comments and Applicability to **Suborbital Aircraft**
Propellant	Fuel or propellant/ oxidiser feed/fuel supply				Major to Hazardous (depending on phase) for SoA; Catastrophic for carrier		Applicable
Propellant	Rocket abort				Catastrophic	Engineering Judgment - additional identified for Suborbital ops	should a non-nominal situation occur (LOC or excessive vibration) then the rocket phase must be able to be aborted to avoid a Catastrophic outcome
Propellant	fuel/propell ant/ oxidiser tank integrity				Catastrophic		Applicable
Fire Risks	Fire risk due to oxygen				Catastrophic		Fire suppression system needs to be considered for closed loop cabin
Other Risks	Unintended SoA - Carrier separation				Hazardous if sufficient height to obtain aerodynamic glide to land; otherwise Catastrophic		Engineering judgment as new technology
Other Risks	Seat Restraint whilst under 'g' force				Hazardous	Engineering Judgment - additional identified for Suborbital ops	Marginal to Hazardous to participants

Table 18: Summary of SoA-specific considerations in the FHA

As detailed in Table 18 the SoA-specific functional failures are centred around the RPS and additional environmentally-driven aspects such as the Reaction Control System, g-force related aspects and the unique aspect of carrier aircraft integration (where applicable by design).

SoA Depth of Analysis Considerations

The depth of analysis flowchart from AC§23.1309 (figure 3 in §23.1309) is a standard process for determining whether quantitative analysis is required or more simple qualitative analysis. The methodology is considered suitable for SoA design organisations to follow.

SoA Assessment of Failure Conditions Probabilities and Analysis Considerations

Although design organisations may follow a safety target approach by using the approach in Table 17 they should apply the implicit safety objectives for the relevant severity classification. However the safety target approach does allow for some flexibility.

(a) *Analysis of Negligible Failure Conditions*: the DO should derive these from the FHA and/or safety appraisal and justify that best practice has been used in the design and to demonstrate independence from other functions.

(b) *Analysis of Minor Failure Conditions*: the DO should derive these from the FHA and/or safety appraisal and justify that best practice has been used in the design and to demonstrate independence from other functions. Additionally the DO should provide an assessment based on engineering judgment from qualitative assessment (and where possible provide quantitative assessment).

(c) *Analysis of Major Failure Conditions*: the DO should derive these from the FHA and from an assessment based on engineering judgment from qualitative assessment (and where possible provide quantitative assessment). The DO should employ formal techniques such as FMEA supported by failure rates and FTA to demonstrate safety of the relevant systems and that redundancy actually exists. The DO should ensure that the cumulative assessment of Major failure conditions is no more than probable i.e. no more than $1x10^{-2}$ pfh in accordance with Table 17

(d) *Analysis of Hazardous and Catastrophic Failure Conditions*: the DO should derive these from the FHA and from thorough safety analysis based on a combination of qualitative and quantitative analyses. The DO should follow the full guidance on the use of tools and techniques as provided in §23.1309. As per the ARAC's analysis on the AC for §23.1309, *any analysis used as evidence that a failure condition is extremely improbable should include justification of any assumptions made, data sources and analytical techniques to account for the variability and uncertainty in the analytical process*. Additionally, the DO should ensure that the cumulative assessment of Hazardous and Catastrophic failure conditions meets the safety targets in accordance with Table 16;

- *Catastrophic* – $1x10^{-4}$ per flying hour
- *Hazardous* – $1x10^{-3}$ per flying hour

SoA Operational and Maintenance Considerations

Operational and Maintenance considerations are dealt with on two distinct levels for these guidelines; firstly from a Safety Management/Safety Analysis perspective and secondly from an operating perspective in terms of flight crew licensing, operating procedures and maintenance factors. The rationale to include the Operational Safety Management aspects is to have an integrated approach within the Policy and guidelines. Indeed EASA are looking to cover not only the airworthiness aspects but aim to start looking at the 'Total System'.

3.3.2 Safety Management Considerations:

Safety Analysis considerations for Design Organisations:

Safety Analysis Considerations for Flight Crew and Maintenance Tasks: These tasks, which are related to compliance (to failure condition's safety objectives), should be appropriate and reasonable; examples of this are pre-flight tests (such as 'Press-to-Test') or selection of a switch to an alternate source (to check for latent failures). Credit can be taken for these design aspects that have a procedural requirement associated with them; in this instance it is reasonable to take full credit because the flight crew/maintainers can realistically be anticipated to perform them correctly when called for and hence a quantitative value of 'one' can be assigned.

Safety Analysis Considerations for Flight Crew Errors: Design analysis (to demonstrate compliance to Failure Conditions) should not include probability values for flight crew error. Should a Failure Condition's safety objective be difficult to achieve then the Designer should communicate this to the certification authority; a Special Condition (SC) may be required. The Designer would also have to

provide qualitative arguments for additional mitigation such as flight crew actions (post the Failure Condition) and possible Limitations and Warnings that may be applied; credit may be taken for this this type of mitigation by the Operator higher in the Accident sequence (see below).

Safety Analysis considerations for Operators:

Operator Accident Risk Management;

Safety Analysis Considerations for Operators: In the case of SoA operations the Designer will inevitably be working closely with the Operator and hence the Operator should continue the analysis from the Failure Condition point (the hazard) to the conclusion of the Accident Sequence. The rationale is that the Accident Risk can be managed more effectively by the Operator by applying Limitations, Warnings, Training and Procedural mitigation that are applicable from the hazard (failure condition) to the accident. The Operator Safety Risk Management should integrate with the Design Organisation Safety Analysis in order to provide a contiguous 'Total System's Approach'.

	Severity (Safety Event)				
Likelihood/Probability	Negligible	Minor (Minor Incident)	Major (Major Incident)	Hazardous (Serious Incident)	Catastrophic (Accident)
Frequent $> 10^{-2}$	**C+**	**B**	**A**	**A**	**A**
Probable 10^{-2} to 10^{-3}	**C-**	**C+**	**B**	**A**	**A**
Occasional 10^{-3} to 10^{-4}	**D**	**C-**	**C+**	**B**	**A**
Remote 10^{-4} to 10^{-5}	**D**	**D**	**C-**	**C+**	**B**
Extremely Remote 10^{-5} to 10^{-6}	**D**	**D**	**D**	**C-**	**C+**
Improbable 10^{-6} to 10^{-7}	**D**	**D**	**D**	**D**	**C-**
Extremely Improbable $<10^{-7}$	**D**	**D**	**D**	**D**	**D**

Table 19: Proposed Operator's Accident Risk Matrix

Table 19 has been rationalised into an Accident Risk Matrix and aligns with Table 17 for the designers' safety target based (failure conditions) risk matrix; the classification also conforms to the ALARP principle to allow for total system risk acceptance/ management. The 'shape' of the risk matrix tends towards the risk-averse because of the immaturity and high-risk nature of the proposed spaceflight activities. The matrix has been 'calibrated' to allow for 100 'arbitrary' critical system's failure conditions per the origins of safety objectives as detailed in AC 23.1309 [87].

The following Risk Acceptance Criteria is primarily for the Operator but can be used for the DO as the Risk Matrix has the same classifications.

Accident Risk Classification	Accident Risk Acceptance and Authorisation Criteria
A	Unacceptable
B	Undesirable but may be tolerable with the authorisation of the Spacecraft Operator's President/Company Board
C	Tolerable. Acceptable with the authorisation of the Safety Panel
D	Broadly acceptable

Table 20: Proposed Risk Acceptability Criteria

Operator Flight Safety Program;

- Flight Safety Program. The Operator should implement a Flight Safety program based upon the Flight Operations and Quality Assurance (FOQA) program. This is standard 'best practice' and involves:
- Risk Profiles. These should be based on severity as well as frequency of occurrences (these can be used to feed back into the Total System Approach mentioned above)
- Occurrence Reporting System; The occurrence reporting system for operators needs to be considered and detailed within the SMP and includes;
  - Air Safety Reports – these are standards reports within a Mandatory Occurrence Reporting scheme. In addition this form may have to be adjusted for the suborbital domain. This is noted as a recommendation at 6.4.9
  - Health & Safety Reports – these are also standard reports for incidents occurred on the ground. Any injuries or accidents in flight should have an occurrence report (as above) in the first instance and then this can be reported in terms of health and safety
- As Low As Reasonably Practicable (ALARP). The FAA guidance [18] does not include ALARP methodology however it is recognised in the ANSI GEIA Standard (Best Practices for System Safety Development and Execution) [84] as well as in the UK. European countries do not employ the ALARP process however countries do use similar processes:
  - France: Globalement Au Moins Aussi Bon (GAMAB) [73]

    This is whereby a new system must offer a level of risk globally as least as good as the one offered by any equivalent existing system

  - Germany: Minimum Endogenous Mortality (R_m), (MEM) [74]

    This is hazards due to a new system should not significantly augment R_m (equal to 2.10^{-4} fatalities/person year)

- Operational and Maintenance Considerations:
- Operational Considerations:
- The main aspect covered in the EASA SoA Policy is in terms of Flight Crew Licensing (FCL)
- Maintenance Considerations:
- The main aspect covered in the EASA SoA Policy will be in the guidance material (section 3.3)

In essence Reducing Risk is a common goal in safety management terms and one that should be applied at the Accident level i.e. for Operators; Design Organisations should continue to apply 'safe design' principles and adopt the safety precedence sequence in order to meet their safety targets (and implicit safety objectives). It is considered that due to the different approaches throughout Europe that

the ALARP process shall not be included in the EASA SoA Policy but will be included in the 'Exemplar Safety Model' in Section 3.4.9. It is discussed here as Operators should be reminded that they should employ a process whereby they (along with the DO) can demonstrate (by some form of cost benefit analysis or similar) that the Risks have been reduced as far as possible; Operators should bear in mind that they would have to produce this as evidence in a court if an accident occurred.

3.3.3 Supplemental Considerations Conclusion

The aim of this section was to provide more detailed guidelines for EASA to consider as supplemental information to support the SoA Policy for both Design Organisations and Operators alike. The section provided explicit severity and probability classifications that would be suitable for DOs and Operators and therefore they would use the same metrics within a contiguous safety model. These categories then formed the basis for the Risk Matrix and Risk Acceptance criterion. To assist the Operators specific Accident Lists were derived based on ICAO standards such that they could continue the accident sequence analysis from the DO through to the concluding accident risks.

The rationale for having these guidelines is to standardise the baseline safety management system components such as Safety Requirements, Safety Targets (and derived safety objectives) and specific, recognised Accidents to which Operators can manage their 'recovery barriers' leading on from the standard failure conditions and hazardous state.

It is concluded that a contiguous safety approach can only be achieved by using common metrics and this is not currently adopted in aviation. The EASA SoA Policy supplemental guidelines can provide this information to assist the nascent suborbital designers and operators in effectively managing the airworthiness and safety of the SoA 'Total System'. The designers should adopt the safety target approach (with implicit safety objectives) as detailed in Table 17 and the operators should adopt the Total System approach as detailed in Table 19. The aim for the operators is then to demonstrate that the Accident Risks are reduced and managed by the use of operating procedures, training and limitations as controls such the Total System Risk (per severity) also meets the safety target and maintains this throughout the life of the system.

3.4. EXEMPLAR SAFETY MODEL – SPACEFLIGHT OR AVIATION

The review sections in Chapter Two highlighted 'best practice' Safety Management Systems and activities and also highlighted some weaknesses (gaps) in both the emerging spaceflight safety methodology and also in the extant aviation-based methodology. The review concluded that the 'best practice' guidelines were bespoke to Design Organisations or to Operators; there was no cohesive approach that could take the base events of the DO analysis (FMECA data) right through the accident sequence to the Operator Safety Risk Management and fed back into the FMECA data to close the loop. This section proposes a 'World Class Safety Model' that is generic enough to be considered for both the emerging spaceflight industry (orbital or Suborbital) and also for the aviation industry; arguably it can also be applied to other Industries where a complex system exists.

3.4.1 Exemplar Safety Model – Cohesive Approach

The current status of analytical approach is considered to be bespoke and this is corroborated by a lack of 'integrated' guidance material. Figure 42 below depicts the current status.

Figure 42: Author's depiction of current safety analysis

To achieve an integrated approach based on the current system requires the DO and Operator to engage more closely so that a closed loop system may be implemented. Figure 43 below shows the relationship that should be considered as standard between the DO and Operator; however as clearly demonstrated in the Case Study at section 3.4.7 this is not the industry standard practice as yet. Moreover, the Operator is not involved in other DO safety activities such as HMI, Systems and Safety Engineering and other useful analysis such as the OHHA and OSHA activities; these latter two in particular are especially relevant to the Operator's hazards as it involves the effects to and caused by the 'front-line' pilots and support personnel. Figure 44 depicts these separate activities and these bespoke activities were indeed the 'norm' on a project that the author has recently been involved with. These activities are, in their own right, extremely important however they are all inextricably linked and more emphasis should be placed on an integrated approach.

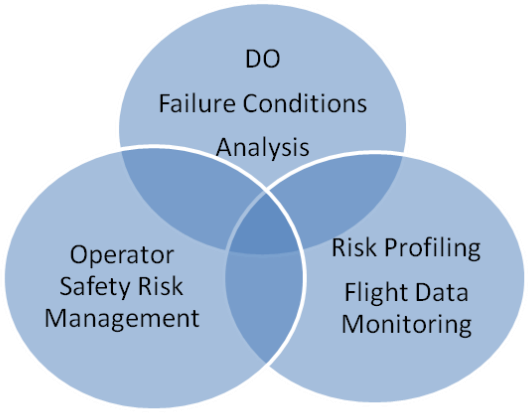


Figure 43: Ideal depiction of safety analysis

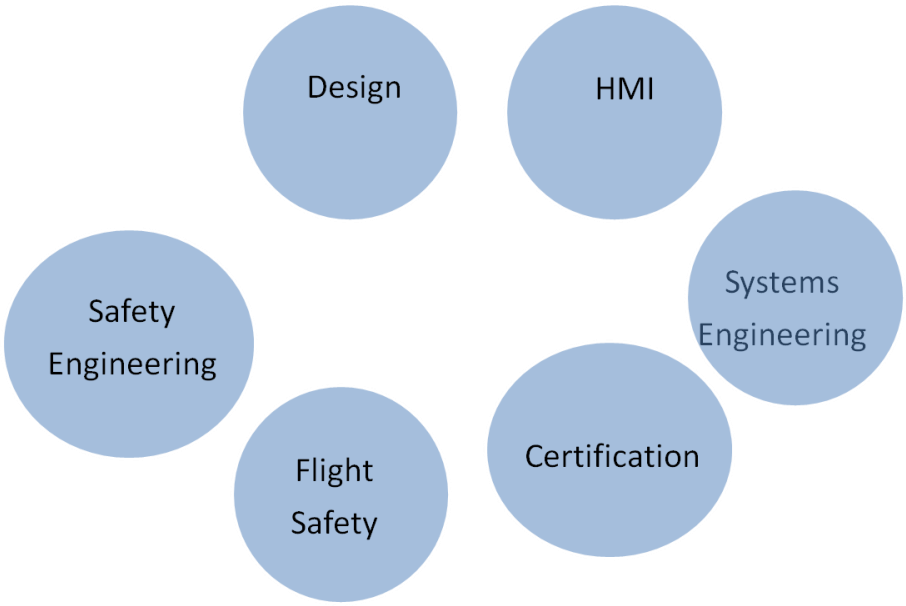


Figure 44: Current aerospace program that the author was involved in (also previous working model for NASA as presented at the 4th IAASS conference)

Figure 45: Proposed Integrated Design, Certification and Safety Model for new projects in the Spaceflight and Aviation domains

Figure 45 is the proposed approach for the suborbital spaceflight domain (and arguably should be applied to all aerospace projects). The approach is that the three main domains (Safety/HMI and Design) should be represented at all meetings in the suborbital airplane design and development lifecycle including the concept, assessment, design, manufacture, test phase through to operations and disposal.

Additionally Operators should be involved at the outset because they will be able to participate in setting 'User Requirements'. Then arguably the Operator community (including pilots and safety manager) should be involved at meetings throughout the project and in particular HMI working groups. In terms of safety management and systems safety engineering, Operators (especially pilots) will be able to contribute towards verification and validation of Fault Trees and in particular in getting the accident sequence correct.

3.4.2 Exemplar Safety Model – The Amplified Accident Sequence

The following figure represents a standard 'Accident Sequence'. This is a simplistic representation and one that includes the consequence (or harm). When considering the basic sequence it becomes clear that it does not represent what the DO achieves (in terms of safety analysis) and it also does not achieve what the Operator does (in terms of managing the operating risks i.e. an Operator's cause may actually be a DOs hazard). As was concluded in the review phase (2.2.17) there is currently no 'joined-up' approach and this was the initial starting point for introducing a new safety model.

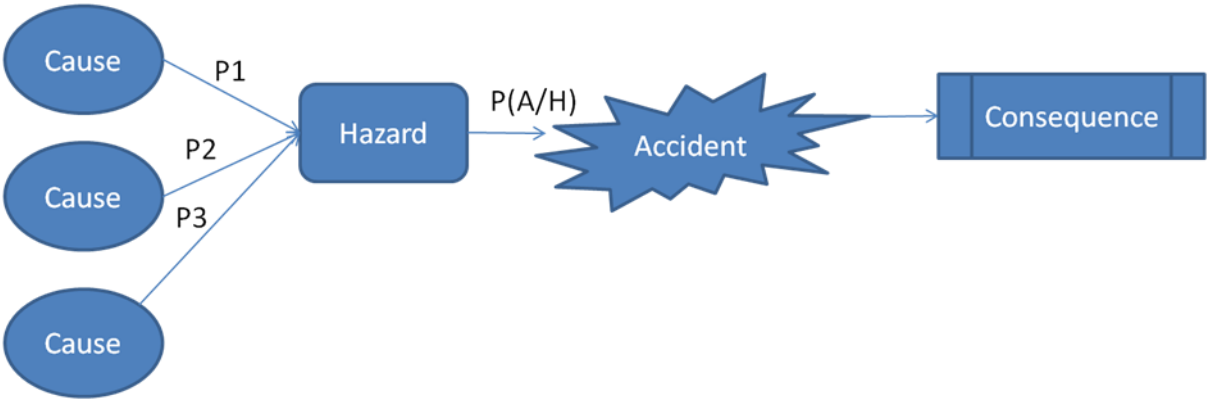


Figure 46: Standard Accident Sequence

3.4.3 Exemplar Safety Model - Construct

The '*SATURN SAFETY MODEL'* attempts to provide a cohesive, full circle sequence that apportions responsibility at the right point and enables Designers and Operators to use the same construct as opposed to current disparate 'best practice'. The model takes cognisance of the best practice guidelines for DOs and Operators and of other theoretical models attempts at providing solutions in the Operator domain. Examples of the best practice and 'other' references include:

- ARP 4761 (for DOs)
- ARP 4754 (for DOs)
- ARP 5150 (for Operators)
- FAA System Safety Handbook (for DOs)
- FAA-AST documents (for launch license operators – this can also mean the designer who is test flying the vehicle under an experimental permit)
- EASA 'ARMS' (for Airline Operators)

The *SATURN SAFETY MODEL'* aims to provide clarity and ease of transition to useful tools such as simple Event Trees and spread-sheets to assist Operators and finally an effective hazard log tool.

3.4.4 Introducing 'Key (Platform) Hazards'

The *SATURN SAFETY MODEL* is derived from understanding the boundaries of the Design Organisation safety analysis and the boundaries of the Operator Safety Risk Management. In Figure 47 below a diagonal line has been inserted to show the boundary between the two functions. From this it is clear to see that the DO is responsible up to the Failure Condition (in order to demonstrate that the airworthiness meets the certification criteria [safety objectives]). The review in Chapter two (2.2.10) detailed that the Operator then undertakes bespoke Risk Assessments and hence the sequence of events (the accident sequence) is not a contiguous representation of causal factor to accident scenario. Although during a subsequent review a 'prime hazard' term was identified in GAIN's Operator's Flight Safety Handbook [33] Appendix E; here the prime hazard was used in an accident sequence that started with 'initiating hazards' and then followed by contributory hazards. Although the sequence was not well constructed and the three levels of hazard slightly confusing the intent of having a prime hazard was noted. This was used in an accident sequence example but not further explained and so there is no further reference to this within the main part of the document.

The *SATURN SAFETY MODEL* construct joins the two disparate safety analyses by means of a 'Key (Platform) Hazard' (depicted as KH in the Operator analysis part). This is the author's initiative and represents a higher-level 'platform' (aircraft/spacecraft) event.

Figure 47 below shows the *SATURN SAFETY MODEL* construct in simplistic form.

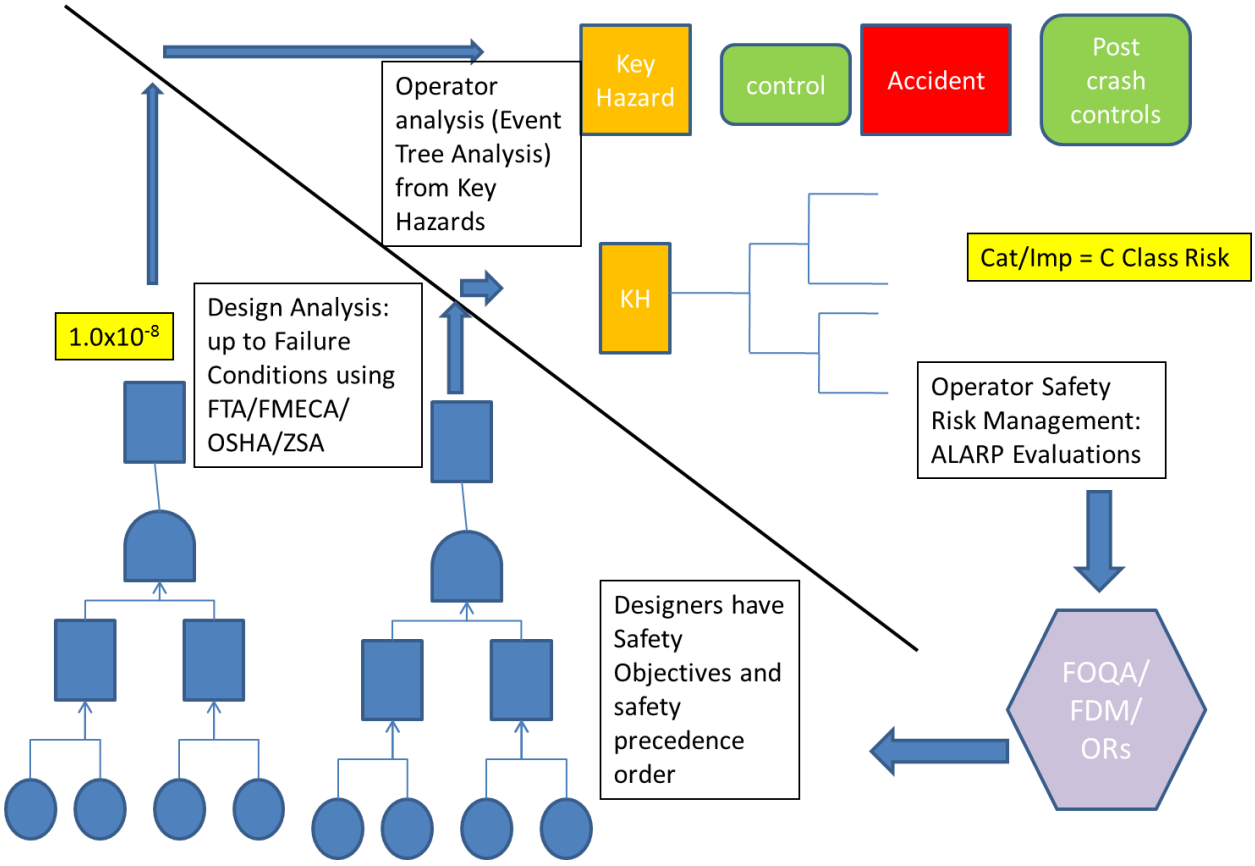


Figure 47: Exemplar Safety Model: DO analysis using Fault Trees up to the Hazard (failure condition), then Operator analysis encompassing Aircraft level Fault Tree and Event Tree, following on to Safety Risk Management and feedback to the base events of the Fault Tree (FMECA data updates)

The Key (Platform) Hazard is derived from the higher-level 'blocks' of a typical FHA's Functional Block Diagram (FBD). Figure 50 below represents an exemplar FBD to determine the key aircraft/spacecraft functions; this can then become useful in determining higher level Key (Platform) Hazards i.e. when a hazardous state truly exists in that moment of time within the sequence. In essence should a failure condition exist then this does not immediately (in most cases) lead to an accident as there may be standard procedural pilot cross-checks that would apply. However should the pilot cross-checks (and training) fail, then a hazardous state will now be present; even then, the following sequence could have an emergency drill and/or training to compensate for the hazardous state in order to prevent the accident. So, in order to be explicit in an accident sequence it is necessary to split the analysis accordingly as in Figure 47 (DO Failure Condition Analysis & Operator Safety Risk Analysis).

It is worth restating the definition of a failure condition:

> *"A condition having an effect on either the airplane or its occupants, or both, either direct or consequential which is caused or contributed to by one or more failures or errors considering flight phase and relevant adverse operational or environmental conditions or external events"*

The definition implies that failures or errors (causes) contribute to a failure effect (the failure condition) which relates to the specific phase of flight within environmental context (exposure for say flying in IMC) that impact on the aircraft (the consequence of the failure condition i.e. catastrophic, hazardous etc.).

Therefore the failure condition (system based hazard) sits at the boundary of the system and interacts with the aircraft boundary with predetermined consequences as depicted in Figure 48 below:

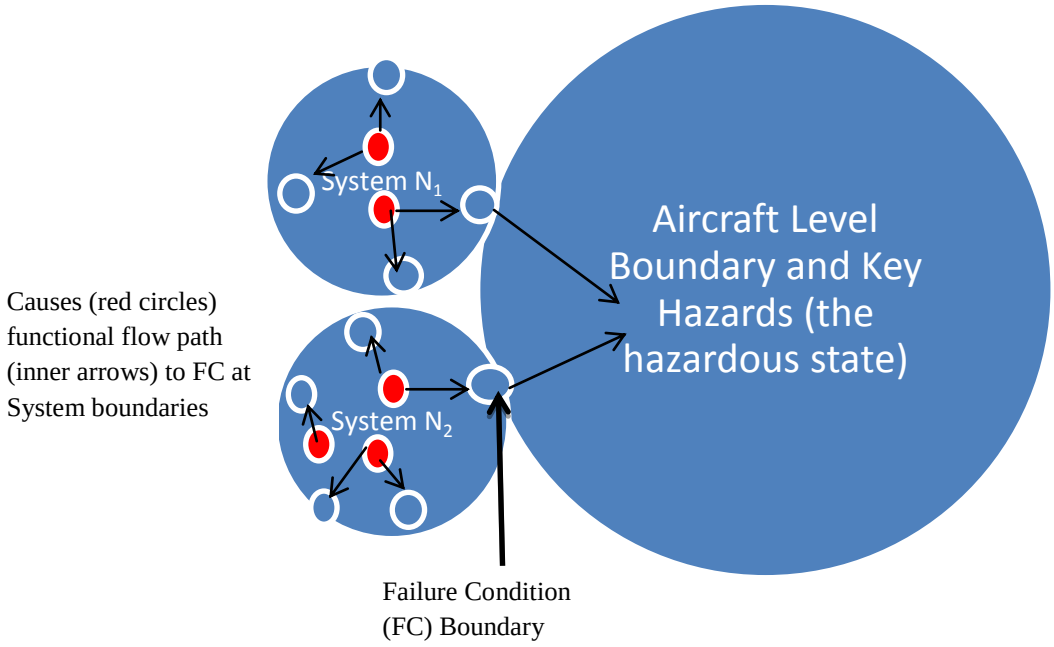


Figure 48: Boundary of Failure Condition to Aircraft Level Key (Platform) Hazards

In Figure 48 we can see that a failure condition (FC) such as '*misleading altimeter'* (determined as a catastrophic FC meeting $1x10^{-9}$ pfh) in itself does not at that moment constitute a hazardous state; it becomes consequentially a hazardous state (key (platform) hazard) when the flight path changes and if the warnings and pilots actions fail to correct the condition. Even then to result in a catastrophic accident would require the aircraft to be near the ground or another aircraft and then still the avoidance system would have to fail or pilot once again not reacting in time. Let us also consider the '*loss of altimeter'* case which is deemed to be a hazardous FC (meeting $1x10^{-7}$ pfh): in this instance the safety margins are reduced and this may lead to a hazardous state per the 'misleading' scenario above; in the explicit *SATURN SAFETY MODEL* we would then link this to a Safety Significant Event (SSE) of Near CFIT and Near MAC (see Table 13) via a Key (Platform) Hazard (the hazardous state). However one could argue that this event could also lead to a catastrophic event though by its probability classification it is two orders of magnitude less likely to result in a catastrophic event.

Here we have found that the FAA/EASA FHA criterion is one-dimensional in the FC to Severity relationship and that a designer could simply model his analysis (by FTA) for each case i.e. a FTA for misleading altimeter to meet $1x10^{-9}$ pfh for the catastrophic scenario and a separate FTA for loss of altimeter to meet $1x10^{-7}$ pfh for the hazardous scenario.

However the *SATURN SAFETY MODEL* contends that by explicitly continuing the sequence via Key (Platform) Hazards up to and beyond the actual accident then it can be proven that the lower severity FCs could be linked via the appropriate Key (Platform) Hazards to its designated severity accident

and also the higher severity accident; this would have to be modelled correctly and the analyst would ask the questions ‘what is the worst possible outcome’ and ‘what is most credible outcome’; then it is a matter of choice as to whether both should be included in the analysis and whether this is practicable and manageable. Figure 49 below details the linking of FCs to Key (Platform) Hazards to either Accidents (Table 12) or Safety Significant Events (Table 13) – note; controls are not shown:

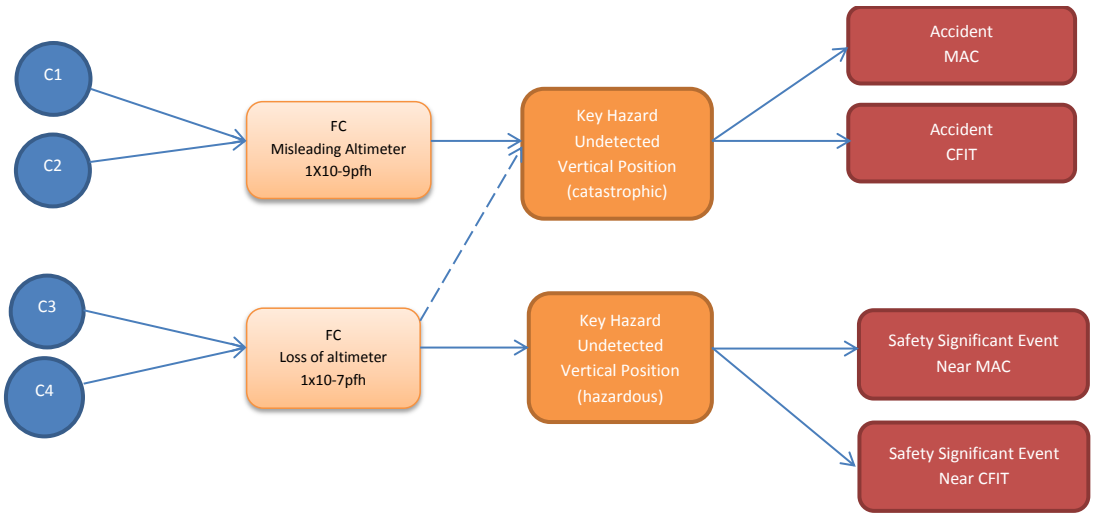


Figure 49: Accident sequence depicting Failure Conditions to Key (Platform) Hazards to Accidents/Safety Significant Events

To continue the supposition regarding lesser severity classifications per failure condition one could argue the following:

Catastrophic FC = 10-9 pfh (target) x 1 (implicit in definition) = 10-9 pfh “Catastrophic severity”

Hazardous FC = 10-7 pfh (target) x 10-2 (implicit in definition) = 10-9 pfh “Catastrophic severity”

Major FC = 10-5 pfh (target) x 10-4 (implicit in definition) = 10-9 pfh “Catastrophic severity”

Minor FC = 10-3 pfh (target) x 10-6 (implicit in definition) = 10-9 pfh “Catastrophic severity”

The above simply states that it is less likely (6 orders of magnitude) that a Minor FC would result in a catastrophic severity scenario and therefore this is why the FCs have a derived severity attached to them; however when the sequence is explicitly detailed as in the *SATURN SAFETY MODEL* the case could be argued for a hazardous FC resulting in not only a hazardous SSE but also a catastrophic accident as depicted in Figure 49; the rationale is that this is within 2 orders of magnitude and could be deemed credible.

The Key (Platform) Hazards are the linking mechanism as these are a component of the aircraft level boundary whereas the FC boundary is still at the system-based level; it is recognised that a system may comprise redundancy i.e. separate display systems supplied from separate sources and have additional safety features as controls but still belong to the *misleading altitude* FC.

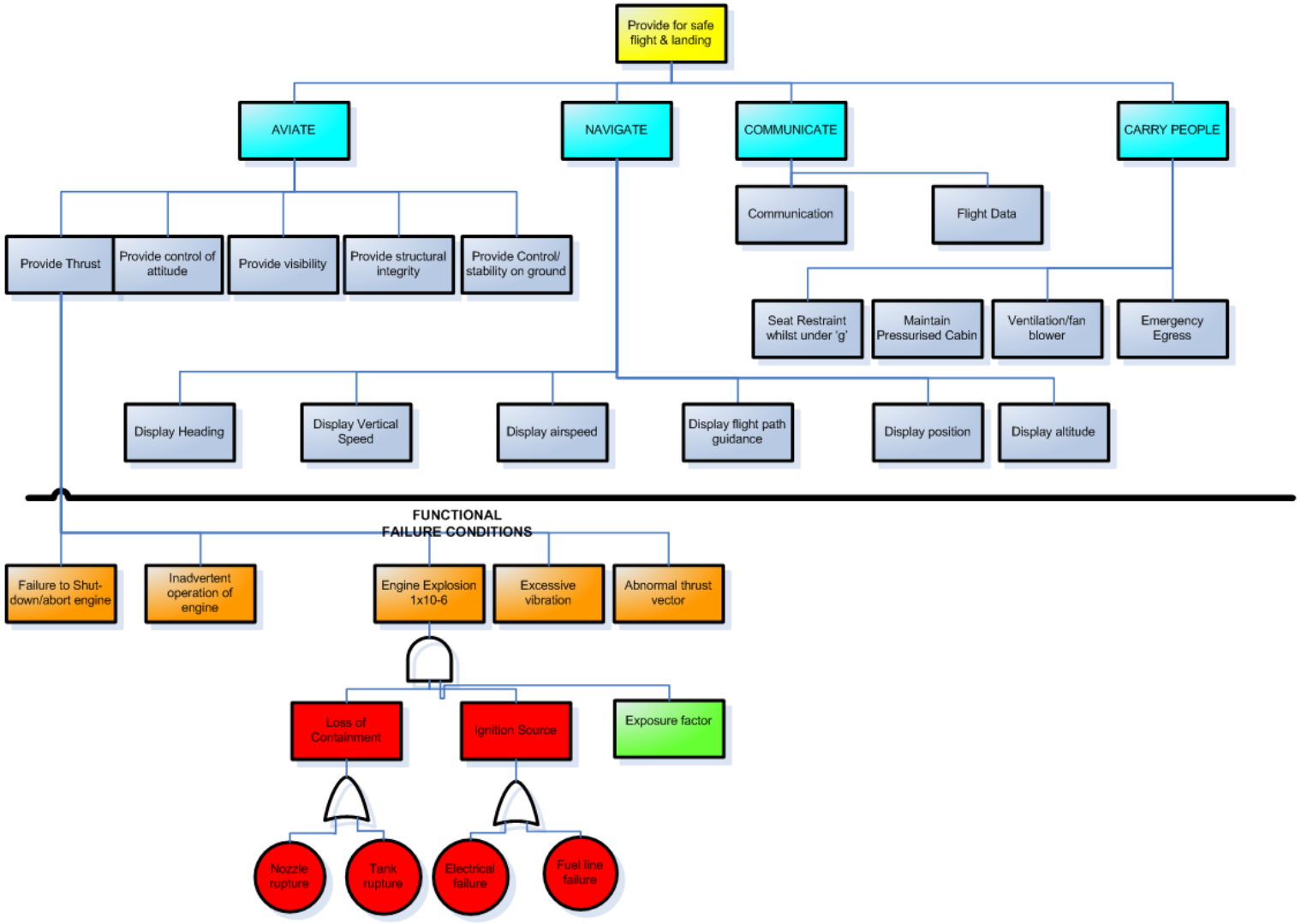


Figure 50: Exemplar Suborbital Spaceflight Functional Block Diagram 1st Level (light blue - Key (Platform) Hazards derived from here) & 2nd Level (Failure conditions)

In order to illustrate the process, the function 'To Provide Thrust' will be examined in terms of a simple FHA approach. Table 21 below contains the results of the high-level FHA. Where the function was deemed to be more suited to a lower-level function this is detailed as 'N/A' (not applicable – more suited to System-level functional failure condition).

Function	Failure Mode	Functional Failure	Effect	Classification	Key (Platform) Hazard (KH) or Lower-level Failure Condition
Provide Rocket propulsion	No	Loss of Propulsion	Rocket stops producing propulsion	Hazardous	Lower-Level Failure Condition leading to KH of 'Recoverable' Loss of propulsion (SSE) Irrecoverable Loss of propulsion (Accident)
	Too much	Power-plant runaway	Rocket produces too much propulsion with possible explosion	Hazardous-Catastrophic	Lower-Level Failure Condition
	Too Little	Insufficient propulsion	Rocket produces insufficient propulsion to complete ascent	Hazardous	As per first line above
	Un-commanded (provided when not required)	Un-commanded propulsion	Propulsion provided when not required which can lead to loss of control	Hazardous-Catastrophic	KH = Loss of Propulsive Control
	Incorrect	Abnormal Thrust Vector	Propulsion provides abnormal vector leading to loss of control	Hazardous-Catastrophic	KH = Loss of Propulsive Control
	Uncontained	Uncontained rocket propulsion	Rocket combustion or propulsion not contained leading to explosion	Catastrophic	KH = Uncontained fire/explosion

Table 21: Exemplar FHA – also used to determine Key (Platform) Hazards

In terms of the *SATURN SAFETY MODEL* at Figure 49, the Key (Platform) Hazard following on from the Failure Condition i.e. *Misleading Altitude* Failure Condition) leads to *Undetected Vertical Position Error* (Key (Platform) Hazard). The Operator analysis takes up the safety analysis from the Failure Condition and therefore the Operator is responsible for assessing the Risk of an Accident (or Serious Incident) occurring and applying suitable mitigation. In this instance to prevent the *Misleading Altitude Display* becoming a platform-level hazardous event (the wrong place at the wrong time for instance) i.e. *Undetected vertical Position Error*, the Operator can instigate a procedural control that ensures the pilots cross-check their instruments with alternate sources. The rationale is that the Failure Condition *Misleading Altitude Display* does not directly lead to an Accident; it requires other factors to be present in the accident sequence and one of those is the direct input of the pilot.

3.4.5 Exemplar Safety Model – Design Organisation Analysis

The DO analysis begins at the Preliminary Hazard List (PHL) derived from the initial safety requirements and preliminary hazard identification activity. Then as part of the analysis process FTAs are produced for each system and sub-system culminating in the Failure Condition as the top event.

3.4.5.1 DO Level Fault Trees

The DO level FTA is necessary to demonstrate compliance to certification requirements i.e. that a catastrophic failure condition has met the safety objective of $1x10^{-9}$ per flying hour (for Part 25 aircraft) and that hazardous FCs have met their safety objective of $1x10^{-7}$ per flying hour

For SoA the guidelines should detail the necessity for DOs to provide Fault Trees as part of their safety analysis to demonstrate compliance to safety objectives. Within Figure 47 it is clear to see that the DO analysis required is to use Fault Trees to determine the failure condition's probability. A Fault Tree is required for each identified failure condition and the DO should be mindful of the overall Safety Target that the safety objectives are derived from; indeed for a Safety Target approach the 100 catastrophic FCs should be summed to determine whether the safety target has been achieved; within the FTA tool the DO will need to provide the separate FC Fault Trees in the combined library and then link the events to the top gate i.e. called 'catastrophic safety rate achieved' or similar. The same must then be carried out for the hazardous and major FCs.

Exposure Factors

The use of Exposure Factors is essential within the Design Safety Analysis as this can then more accurately reflect the nature of the failure condition and therefore its contribution towards the accident. Figure 51 below shows an exemplar Fault Tree construct for the Failure Condition 'Engine (rocket) Explosion' incorporating the exposure factor (X-FACTOR) for the rocket phase; in this instance the X-FACTOR has been set to 90 seconds of a 1-hour flight. As can be seen this has a positive effect on the probability of the engine explosion in the sequence and this will assist the DO in attempting to meet the required safety objectives or safety target.

Special Conditions (SC) may have to be applied for SoA in that it is widely known that typical 'rockets' achieve in the order of $1x10^{-4}$ per flying hour failure rate. This is why that it is so important to model the exposure factor (time for rocket burn) into the FTA. As the catastrophic safety objective (for example $1x10^{-8}$ per flying hour) will not be achieved then this will have to be declared by the DO to the authority i.e. EASA. However, the next step is for the DO to be able to (in the first instance) demonstrate that the 'trade-off' between other well-proven systems (such as the landing gear) will have more than met their safety objective and so the overall Safety Target (for Loss i.e. catastrophic) is still met. Should this not be the case then the DO must discuss with the Operator to take credit for some of the Operator Risk Reduction measures such as Limitations and Operating Procedures; these will bring the probability down to a 'Tolerable' level to allow for certification.

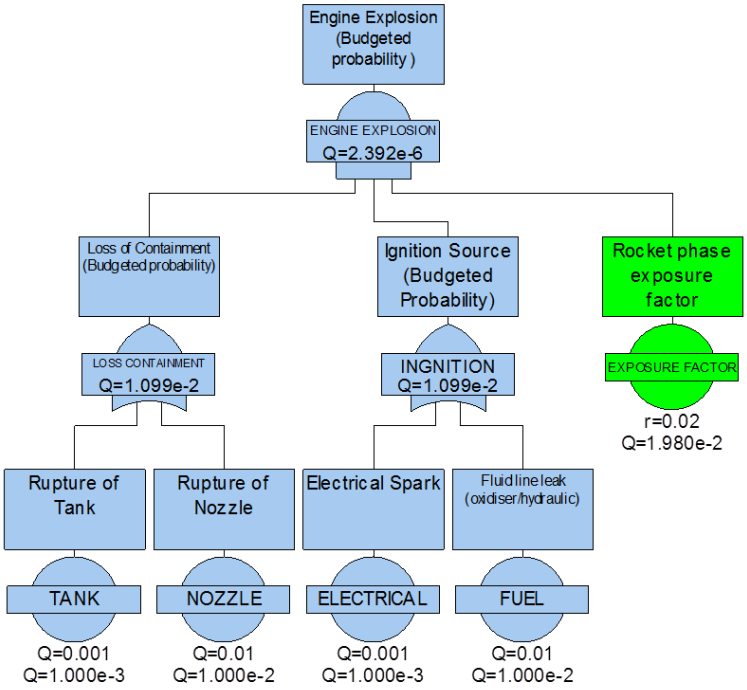


Figure 51: Example use of FTA with the Exposure Factor ANDed

3.4.6 Exemplar Safety Model – Operator Safety Risk Management

The review of Operator Safety Risk Management highlighted shortcomings in that Risk Management was conducted on an occurrence-based need i.e. based on the highest number of occurrences in the FOQA Risk Profile chart. In order to be more effective and understand the spacecraft/aircraft Individual Risks (per Accident or SSE) and also the Total Risk, Operators need to undertake high-level safety analysis using both prospective and retrospective and diverse techniques. The proposed technique is using a combination of Fault Tree or Event Tree Analysis and by managing the failure of controls (based on occurrences/Air Safety Reports):

Aircraft Level Fault Tree

The aircraft (SoA) level FTA contains the consolidated failure conditions (presented by the DO) and provides the ability to display (on separate Fault Trees) the sum of;

- catastrophic failure conditions
- hazardous failure conditions
- major failure conditions

These top gates in these Fault Trees can then arguably be summed (presuming independence) to arrive at the Total System Risk (Section 3.4.10). However it is also important to be able to show the catastrophic Accident FTAs only in order to demonstrate compliance to the **design Safety Target** (for Loss of the platform) for certification.

Aircraft Level Event Tree

The above FTAs created by the DO were summed to determine whether the safety targets had been achieved. That is the first step towards certification within an EASA regulatory framework. Then the Operator continues the sequence via Key (Platform) Hazards to the accident and beyond

(consequences). This can be done using FTA or using an Event Tree Analysis (ETA). The aircraft (SoA) level ETA takes the DO failure condition title as the 'initiating event' and models the controls (and failures thereof) to verify the accident probabilities and also to identify further controls (including post-crash/post event controls).

Human Error Controls

Credit can be taken for Pilot Procedural aspects, however this must not be taken as credit within the DO FTA; instead this should be applied as controls within the Operator FTA/ETA (see section 3.4.6.3 below).

3.4.6.1 Safety Risk Management

As opposed to the EASA 'ARMS' tool, which has an Event Risk Classification using a bespoke risk classification scheme and then another Safety Issues risk assessment scheme, the *SATURN SAFETY MODEL* focuses on the combined Safety Risk (stemming from a failure condition/hazard) and also provides a step to examine the control(s) that failed; the ARMS tool discounts those controls that failed and concentrates on those that were (likely) to be successful. Additionally the methodology is based on sectors. There are problems with this approach: the first is the use of sectors as this does not correlate to flight hours; the second is that the estimations may not be conservative enough (as they do not relate to human error analysis) and therefore the resultant 'risk' may be biased towards a lower value hence hiding the real risk. Within the Event Risk Classification matrix the metrics have been derived from accident data and appear irrelevant and based on aircraft loss values.

3.4.6.2 Managing Occurrences

Managing occurrences is an essential part of Operator Safety Risk Management.

When an event occurs and is reported (as an Aircraft Safety Report [ASR]) the Operator's Safety Manager must log the occurrence and try to analyse it. This is part of their standard Flight Operations Quality Assurance (FOQA) system. This involves:

- Identifying the Hazard
- Logging it on their Risk Profile system
- Undertaking risk assessments on those aspects that have the highest frequency (the top bars in the risk profile) or those with the highest severity; the aim would be to have a combined profile scheme combining frequency of the occurrence and the severity.

Integrating Occurrences into the Safety Model

Normally this is where the Operator stops (after conducting his Risk Assessment after identifying a 'high-hitter' on the Risk Profile) and also the Design Organisation should then determine whether they have airworthiness issues (reliability issues with components/sub-systems) which may result in modification action; once they have addressed this then they invariably stop there as having done their part.

The *SATURN SAFETY MODEL* requires the Operator Occurrence to be fed back into the Design Organisation analysis in order to determine whether the Contributing Cause (and hence Failure Condition) probability has increased which may in turn increase the likelihood of a Key (Platform) Hazard and in turn increase the likelihood of an Accident or SSE. This is the 'Feedback System' and needs a two-pronged approach as detailed in 3.4.6.3 below.

3.4.6.3 Exemplar Safety Model – Feedback System

Feedback of SSE occurrences: These SSE occurrences are reported in the form of ASRs (and this is concurred as a best practice method of reporting) however additional information/action is required for the *SATURN SAFETY MODEL*:

(a) Update to phase of flight to include:

- Launch
- Rocket Initiation
- Space Segment
- Re-entry from Space Segment
- New Section in Air Safety Report to detail:
- Control Failure; here the question is asked on which of the following failed;
  - Operator Procedure failure
  - Lack of Training/Experience in event
  - Limitation breached
  - Standby Equipment failure
  - Warning System failure
- Contributory Causes;
  - Functional Failures – to the DO base events to back up/add to the FMECA data
  - Human Factors – to the Operator Safety Risk Management section of the Hazard Log

As can be seen the ASR requires updating for the suborbital domain needs and to incorporate the suborbital flight phases and also to incorporate the analysis of failed controls and the equipment/human error causes of the event. This is captured in the recommendations section 6.4.9.

3.4.6.4 Exemplar Safety Model – Analysis of Controls

When an event occurs we must first examine the accident sequence to determine if the cause and hazard exists or whether the event is a new cause or hazard which needs to be entered into the hazard log and analysed further. Once this is achieved we can then determine the Controls within the accident sequence; both 'Defence 'A' (avoidance barriers) and Defence 'B' (recovery barriers or Risk Reduction controls) as depicted in Figure 3; Haddon-Cave's analysis of the Nimrod Accident.

The key is to analyse which of the existing failed controls in the sequence i.e. to identify the control(s) that was not effective. To do this the analyst must first have defined the controls properly and in the hazard log these should be given a status i.e. implemented or if not implemented then perhaps 'active'. The controls are as per the fail safe design concept detailed in AC25.1309 [51]:

- *Eliminate the hazard*
- *Reduce the likelihood*
- *Reduce the severity*
- *Implement safety features*

- *Implement Warning Devices*
- *Provide procedures*
- *Provide Training*

In practical terms these can be grouped as follows:

- Design control; the system design analysis should follow the fail-safe design philosophy and also identify safety-critical systems. In order to design a safe system and to meet failure condition's safety objectives the designer will incorporate;
- Redundancy
    - Hardware
    - Power Supplies
    - Sensors
    - Software
- Procedural Control
    - Flight Crew
    - Maintenance/support
- Training
    - Flight Crew
    - Maintenance/support

Quantification of Operator Controls

The review in 2.2.8.2 derived human error probabilities for operator-based controls from a comparison of human error probability methods and aligning it with Reason's take on Rasmussen's Skill-Rule-Knowledge Based performance levels:

- Control measures for high Stress emergency situations = 2×10^{-1}
- Control measures for well-rehearsed procedures to prevent a hazardous situation = 5×10^{-2}
- Control measures for simple routine operations = 3×10^{-3} per flying hour
- Training for normal procedures = 0 i.e. no additional credit
- Emergency Training = 2×10^{-1} per flying hour based on the high stress situations
- Limitation = = 1×10^{-2} per flying hour based on the general omission error where care is required or general error of supervision

Additionally the review examined a Functional Resonance Accident Model (FRAM) whereby the model re-classifies failures and 'errors' to variability in performance and encompasses an alternative approach to capture the *dynamic nature of how events occur*; to use *resonance rather than failure*. Within the model the man and machine are considered part of the system.

Figure 52 below takes the basic construct of the model and tries to advance it in terms of defining the quality margins and span of control as specific human error rates. Here the modified FRAM suggests that the higher within the accident sequence the event occurs or the pilot enters a high stress situation due to external factors then the more likely he is to make a mistake when carrying out a procedural control.

Additionally the model suggest that during nominal situations that external factors can also influence the performance of a pilot such as managerial (organisational) factors; in this instance the pilot may be more prone to errors during simple routine operations i.e. 3×10^{-3} per flying hour.

The thick dotted line represents an accident sequence whereby the pilot errs during the simple routine operation and then this is amplified by other factors such as equipment failure and or environmental

aspects and it can be seen that this could lead to a stressful situation (as in the Air France AF447 accident) whereby the resonance becomes out of control with possible loss of the aircraft.

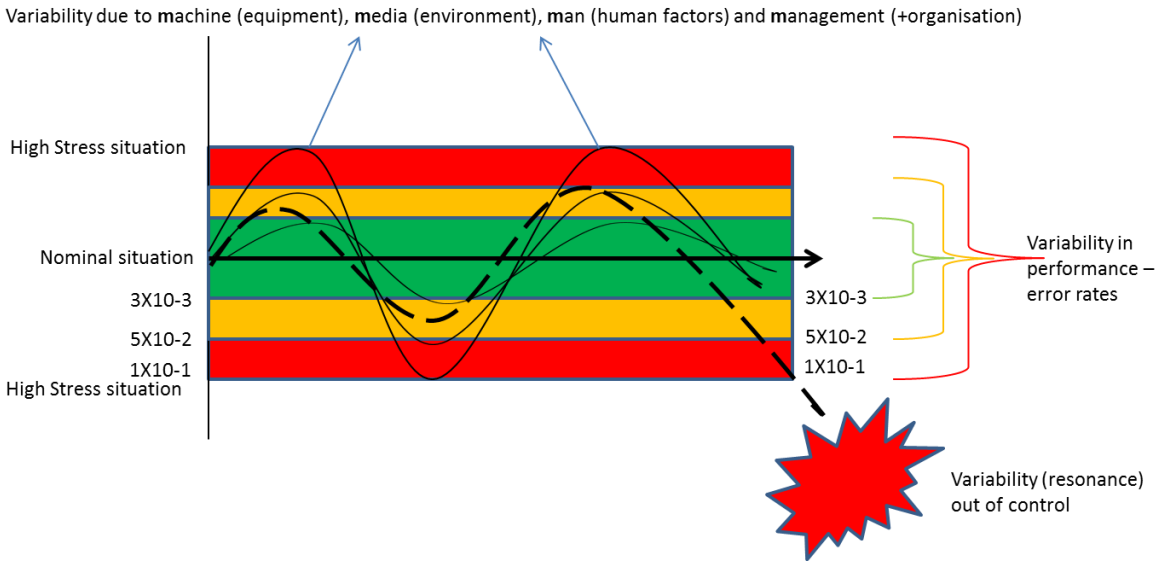


Figure 52: Modified Functional Resonance Accident Model –includes quantitative error rates

Identification of Failed Controls

The Safety Manager should be able to identify which of the controls has failed in the accident sequence and then be able to take appropriate action to try and prevent the occurrence happening again.

Figure 53 below details the different types of control in specific order within the proposed Safety Model; the model integrates the Fault Tree Analysis approach (to determine failure condition probabilities) with an Event Tree Analysis approach (to determine the operator-based controls and their effectiveness). The controls should then been given a probability of success (and failure) in the Event Tree Analysis based on the strength of the control in preventing an accident and in line with the quantitative values for human error described above:

- Preventative controls (avoidance barriers) i.e. design-related up to the failure condition;
- C1 – Standby Displays (for instance); these have probability values within the DO Fault Trees and therefore credit is taken towards the Failure Condition's probability
- Recovery controls i.e. procedures and training and limitations – but also some design controls LHWS/TCAS
- C2 – Pilot cross check of instruments; measures for simple routine operations = 3 x 10^{-3}per flying hour
- C3 – Pilots trained to conduct cross checks and interpret results to make informed decisions = 0 (no additional credit)
- C4 – Design control immediately before accident such as a collision avoidance system or stall warning and assisted recovery system = probability based on reliability of equipment
- C5 – Emergency drill = 2 x 10^{-1}
- C6 – Emergency training for the immediate action drills = 2 x 10^{-1}
- C7 – Limitation = 1 x 10^{-2} per flying hour based on the general omission error where care is required or general error of supervision

Within the Operator's Event Tree Analysis the initiating event would be the Failure Condition and this has a known probability.

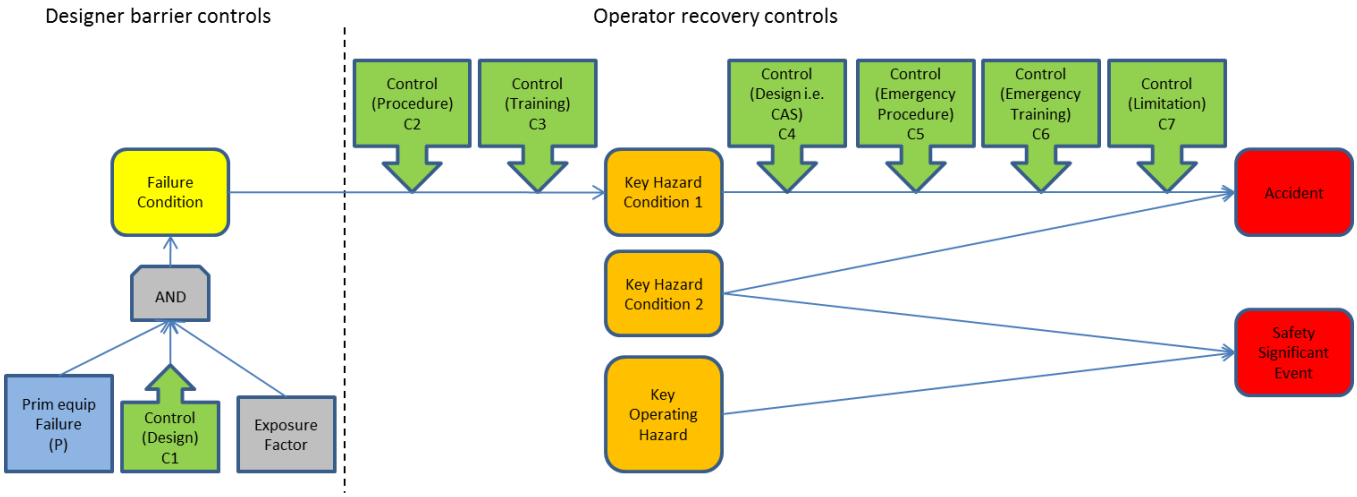


Figure 53: Accident Sequence showing specific controls (design, procedural, training and limitation)

From the sequence in Figure 53 we can see that in order for an accident to occur would require the prime equipment (system) to fail, failure of the operating procedures (to use the design [redundancy] control) which then leads to the Key (Platform) Hazard (hazardous state) and finally failure of any emergency procedures, lack of training and/or breach of any limitations. This was explained earlier in a 'step-through' of a sequence by 'failing' various equipment and controls as was postulated in the Air France AF447 accident. As well as identifying quantitative probabilities for human error as described previously and linking these to variables in performance (modified FRAM above) it is considered necessary to provide these with a weighting scheme in order to quantify the priority of the safety precedence sequence and the operator-based controls. These Risk Reduction methods (controls) are an important part of the ALARP evaluation.

As detailed above, section 2.2.4 suggests that the OSHA activity is one method that addresses operating and support procedures. The OSHA model should provide a sequence of activities to analyse; it is up to the analyst how far back and how far forward he goes (from the actual flight) when analysing the procedures. From the author's knowledge of working with a Design Organisation, they were only interested in analysing the equipment specific elements of the OSHA sequence model. It is hypothesised that the Operators would also only be interested in their Operating procedures and likewise the Support Services (including maintenance) would only be interested in their Support procedures.

In the 'Swiss-Cheese' model below, we are analysing the 'Controls' (the barriers or defences in depth) from the design aspect through to the operations and support aspects; the rationale is that the author wanted to focus on the Safety Model boundaries. In Section 6.4 a recommendation is made for future research into extending the boundaries of the Safety Model to include OSHA sequences that go beyond the immediate aircraft Risks by analysing the other engineering and managerial (Organisational) support aspects; these are the Socio-Theoretical aspects in Leverson's STAMP model [36] as described in 2.2.6.4.

In the model below we are looking for BOTH 'Latent and Active' failures by employing the OSHA technique.

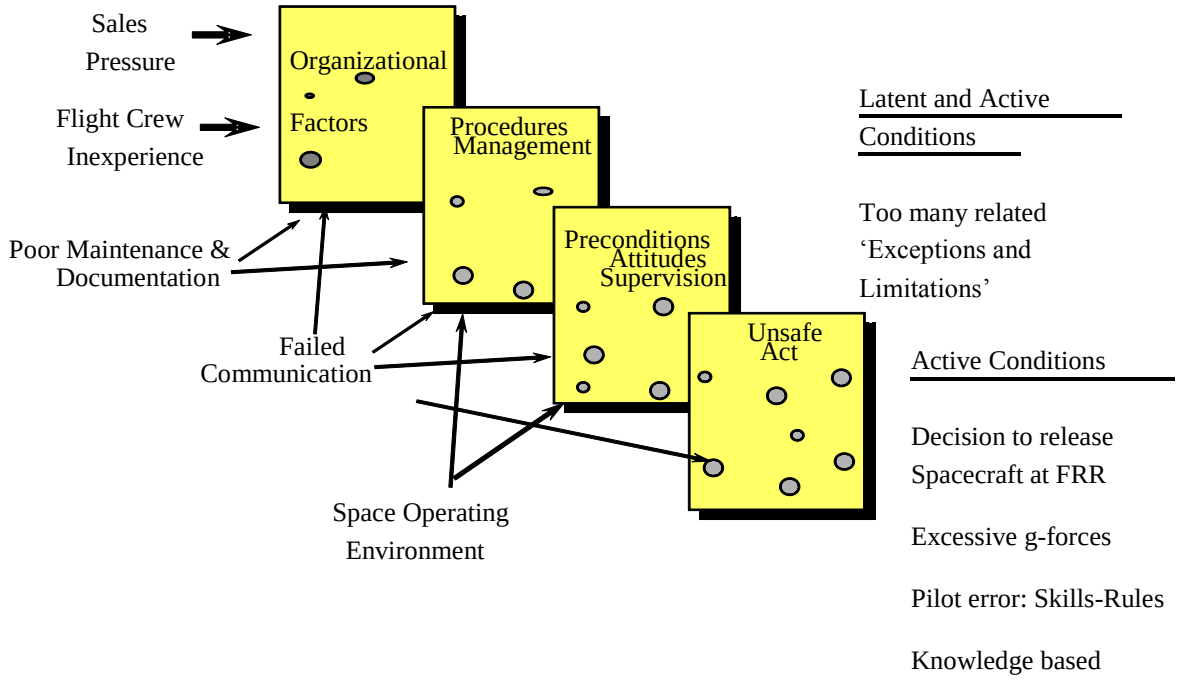


Figure 54: Spaceflight Accident Sequence with 'Active & 'Latent' failures

Integrated Approach Analysis

The *SATURN SAFETY MODEL* links the DO failure conditions/hazards to the Operator Safety Risks in order to have an explicit and integrated sequence of events that can be managed more effectively. The following example step-through shows how the various controls interact (DO controls and Operator controls) in an attempt to assure safety of the SoA/spacecraft:

(a) Risk of Accident with all systems working;

1. Prime System 'Serviceable ('S') – $1x10^{-4}$
2. Standby System 'S' – $1x10^{-4}$ (this is a Design control)
3. Exposure Factor (if applicable) – $1x10^{-1}$
4. Current Status of Total System = $1x10^{-9}$ pfh (catastrophic failure condition reached for Part 25 aircraft)
5. Operating Procedure (normal) control (pilot) – $3x10^{-3}$ (failure rate for human error under normal well practised drill)
6. Training (normal) control – set to 0 (implicit within a normal procedure)
7. Current Operator Risk of Accident = **$3x10^{-12}$ per flying hour**

Now we will see the effect of a prime system failure;

- Risk of Accident with;
  1. Prime System 'Un-Serviceable ('U/S') – 0

2. Standby System 'S' – $1x10^{-4}$ (this is a Design control)
3. Exposure Factor (if applicable) – $1x10^{-1}$
4. Operating Procedure (normal) control (pilot) – $3x10^{-3}$
5. Training (normal) control – set to 0 (implicit within a normal procedure)
6. Updated Status with unserviceable prime item = **$3 x10^{-8}$ pfh** (catastrophic failure condition for Part 25 aircraft now breached but operating procedures AND training are in effect and credit is taken, therefore the aircraft is still safe i.e. the likelihood of a catastrophic Accident is still 'extremely remote' even with a primary system failure and a successful normal drill carried out)

- Risk of Accident with prime system failed and the first levels of recovery controls failed i.e. the pilots did not carry out the normal operating procedure (per the AF447 accident [see case study summary at section 3.4.7]);
  1. Prime System 'Un-Serviceable ('U/S') – 0
  2. Standby System 'S' – $1x10^{-4}$ (this is a Design control)
  3. Exposure Factor (if applicable) – $1x10^{-1}$
  4. Operating Procedure (emergency) control (pilot) – 2×10^{-1} (failure rate for human error under emergency drill)
  5. Training (emergency) control – 2×10^{-1} (author's considered engineering judgement for credit to be taken for training)
  6. Updated Status = **$4 x10^{-7}$ pfh** (catastrophic failure condition for Part 25 aircraft now further breached but emergency operating procedures AND emergency training are in effect and credit is taken (in the negative sense for a Loss Model), therefore the aircraft is still safe i.e. the likelihood of a catastrophic Accident is still 'extremely remote' even with a primary system failure)
- Risk of Accident with prime system failed and second levels of recovery controls failed i.e. the pilots did not carry out the emergency/operating procedures/training (per the AF447 accident [see case study summary at section 3.4.7]); ;
  1. Prime System 'Un-Serviceable ('U/S') – 0
  2. Standby System 'S' – $1x10^{-4}$ (this is a Design control); arguably in this instance (AF447) a design control was the 'stall' system which worked but the pilots did not apply the appropriate technique
  3. Exposure Factor (if applicable) – $1x10^{-1}$
  4. Operating Procedure (emergency) control (pilot) – set to 0 no credit taken
  5. Training (emergency) control – set to 0 no credit taken
  6. Updated Status = **$1 x10^{-5}$ pfh** (catastrophic failure condition for Part 25 is now considered to be probable), therefore the aircraft is not safe and in terms of Risk Acceptance the situation is 'Unacceptable'.

The relevance of the above sequences and explicit realisation of the emerging situation is often not considered because of the disparate safety analysis i.e. the DO tends to stop at the failure condition (having met the safety objective) and the operator does not know the risk probability of the continued sequence with operator controls. When broken down in this manner it is clear that an unacceptable Risk is derived and hence the controls should be strengthened or new controls implemented (such as Limitations).

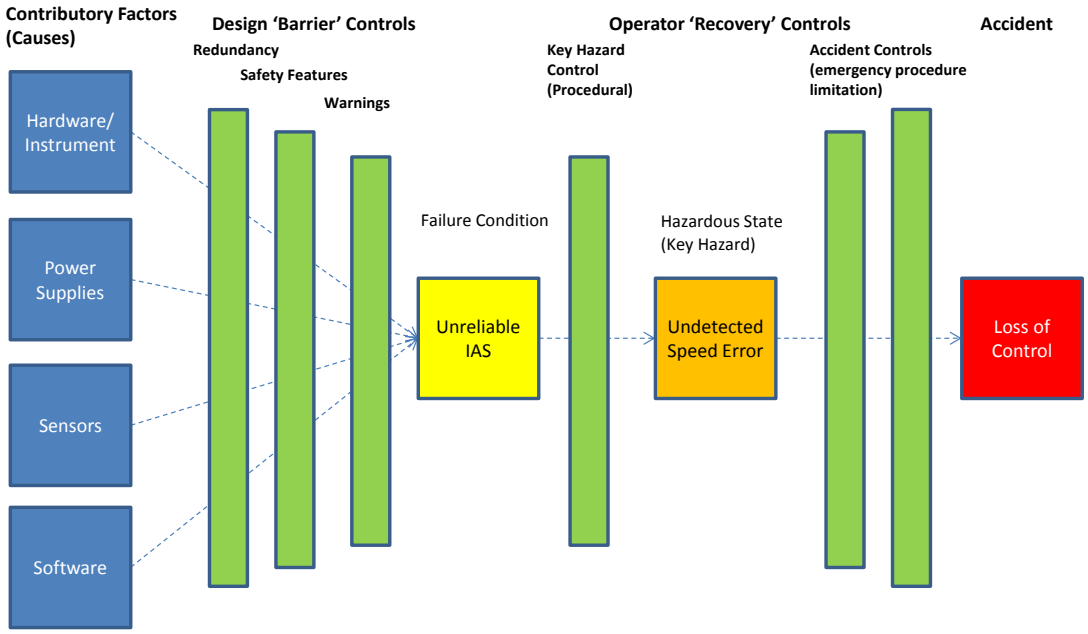


Figure 55: Saturn Safety Model – Generic Sequence detailing Design Controls & Operator Controls with Key (Platform) Hazard Introduced

3.4.6.5 Exemplar Safety Model – Strengthening & Implementing Controls to Reduce Risk

When an occurrence is considered a Safety Significant Event (SSE) then arguably the associated Accident Risk may have increased. Operators (and DOs) should then work to try and reduce the Risk and to ensure that a failed control is strengthened or a different control is implemented as required. The safety model at Figure 55 depicts the accident sequence helps to map out the barrier controls versus the recovery controls.

- STEP 1: IDENTIFICATION OF FAILED CONTROL(S): analyse the Air Safety Report and note;
- Causes; it is important to analyse the described 'event and cause' section of the ASR

  Equipment – if the prime equipment failed did the back-up work?
  Human – note if the equipment was working and the cause was due to the pilot (determine if this is a general lack of skill or actually a skill-based failure i.e. the procedure was not followed correctly); in the latter case note this as a failed control
  Environmental – note if external factors played a part such as icing, wind-shear etc.
- Controls; list the design and operator controls in a logical order

  Design;
  List the standby system equipment
  List the safety features
  List the warning devices

  Operator controls;
  List the normal procedures
  List the specific training
  List the emergency procedures
  List the emergency training i.e. simulator sorties

List the Limitations

Once this causes and controls are listed then the safety manager (with the assistance of a pilot) can examine and pinpoint which control(s) failed i.e. if a fault is enunciated to the pilot did he follow the correct procedures.

Additionally could a Limitation been implemented i.e. in the case of the Air France AF447 accident had a Limitation been imposed (of not flying through icing conditions or not flying at altitudes with super-cooled icing conditions – thus resulting in extra fuel required) then the accident would not have occurred.

- STEP 2: STRENGTHENING OF FAILED CONTROL(S); once the failed controls are identified from Step 1 above the safety manager and pilot should determine whether any of these need strengthening as follows;
- Design:

  Improve the reliability of the standby system equipment
  Implement a new safety features
  Implement a new warning device
- Operator controls:

  Amend or re-brief normal procedures
  Amend the specific training or ensure pilots are trained more often
  Amend or re-brief emergency procedures
  Amend the emergency training or ensure pilots are trained more often
  Add a Limitation or change and re-brief the existing Limitation

- STEP 3: SHOW THIS ON THE WATERFALL DIAGRAM; the safety manager should detail the existing risk and the resultant risk for each stage of strengthening the controls (this may need to be shown over time because procedural controls can be managed/implemented quickly but design changes take time)

- STEP 4: DOCUMENT THIS IN THE HAZARD LOG; the safety manager should record the above in the hazard log and determine whether the accident probability has changed as a result of the failed equipment, failed controls and the introduction of any new or improved controls.

A Waterfall diagram can be useful to show the existing level of Risk followed by the Risk as a result of a serious event. Then the proposed Risk reduction is detailed over an appropriate timescale.

Figure 56 shows a tolerable level of risk (say for an individual accident of Loss of Control) and a new risk being identified i.e. a pitot-tube issue. A design organisation would initiate a Service Bulletin due to the fault but where does that leave the operator (instantaneously) in terms of risk? The designer normally gives a time period for implementing the SB but in the case of Air France AF447 they were still flying ten days after the issue of the SB (to change the pitot-tubes). The operator should have reviewed the previous occurrences in a 'Hazard Review Board' with the safety manager, chief pilot and design representative as a minimum. Then they could have used 'steps 1 and 2' above and identified the following control failures:

- Design Control failures:

  Redundant system failures – design organisation issued pitot-tubes
- Operator Control failures

Amend or re-brief normal procedures (this has now been done by Air France)
Amend the specific training or ensure pilots are trained more often (this has now been done by Air France)
Amend or re-brief emergency procedures (this has now been done by Air France)
Amend the emergency training or ensure pilots are trained more often (this has now been done by Air France)
Add a Limitation – this was not done and is not required now because the design control has effectively reduced the risk

These could be plotted on the Waterfall diagram to show proactive safety management in dealing with the risk whilst awaiting the design to be fully implemented (across the fleet).

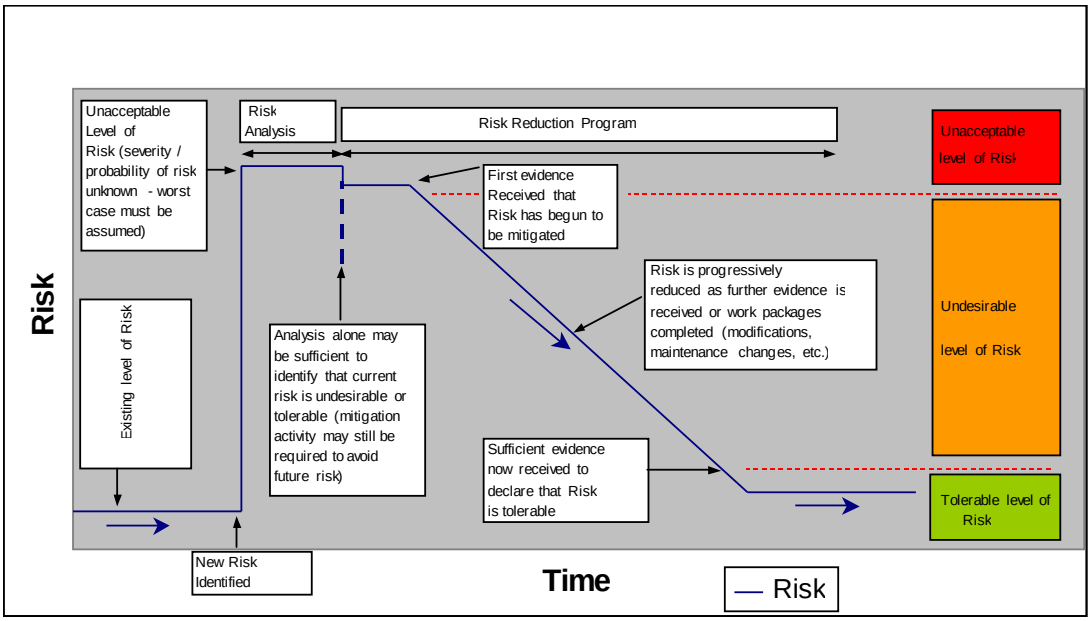


Figure 56: Typical UK MoD Project Team Safety Risk 'Waterfall' diagram depicting the change in Risk due to a Safety Significant Event and subsequent mitigation strategies

3.4.7 Case Studies

To illustrate the reasoning for such a strategy the Air France flight AF447 & Space Shuttles Challenger & Columbia disasters are examined from the 'Saturn Safety Model' perspective and presented at Appendices 3 & 4 respectively.

3.4.7.1 Case Study Summary – Air France Flight AF447 Disaster

On 01 June 2009, Air France (AF) Flight 447 crashed into the Atlantic Ocean en-route from Brazil to France. The Accident is still 'Under Investigation' because the Accident Data Recorder (the black box) has yet to be found. This case study builds on the current facts that are known from the BEA Interim Reports No.2 [91] and No.3 [92].

The Case Study of the AF447 disaster is representative of the disconnect that exists between Design Organisations and Airline Operators. The author acknowledges that they do communicate, particularly in the form of Service Bulletins (SB) when a Safety Significant Event (Serious Incident) requires changes to design or procedural/maintenance inspection strategies (as per the TWA flight 800 that resulted in Special Federal Aviation Regulation 88 requirements and subsequent SBs).

The Case Study shows that previous Serious Incidents (from the Automatic Communication Addressing and Reporting System [ACARS]) resulted in SBs concerning a new design for the pitot-

tubes yet Air France were still flying aircraft with the standard pitot-tubes; the issues highlighted in the Case Study include:

- Known Issues
  - ACARS – previous flights etc.
  - SBs raised, some Operators implemented others not (Cost versus Safety? i.e. to cancel cross-Atlantic flights would be costly and this may have been a factor in the management's decision to keep flying)
  - AF447 – ACARS and flight crew not experienced/trained; the Captain was on a rest period and two co-pilots were flying
- Complacency
  - Management is terms of lack of urgency towards SB
  - Flight Crew procedures and training; Examination of their last training records and check rides made it clear that the co-pilots had not been trained for manual airplane handling of approach to stall and stall recovery at high altitude [92]
- Lack of (Safety) Risk Management
  - No mitigation undertaken by Air France
    - Training – simulator training for *Unreliable IAS* should have been carried out immediately on receipt of the SB and formal analysis by the Air France Safety Manager
    - Procedures; the Chief Pilot should have revised the procedures for *Unreliable IAS*
    - Limitation; limitations should have been imposed on Transatlantic flights;
      - Flights limited to <31,000ft (FL310) or that determined not to be susceptible to super-cooled conditions – this would mean carrying extra fuel/less payload
      - Flights in or near Cumulonimbus clouds forbidden – once again this may mean carrying extra fuel to divert around these clouds (on the night other aircraft diverted up to 90 miles around these sort of clouds in the area)

In essence, by using a properly constructed 'Safety Model' and using an ALARP Evaluation process, the Operator should clearly understand the Accident Risks presented by their aircraft and its operations. One this is determined the Operator can then know explicitly what Avoidance Controls and Recovery Controls are linked to specific Accidents and Key (Platform) Hazards. Thus, when a Safety Significant Event occurs the Operator's Safety Manager will be able to reference the SSE contributory factors into the 'Safety Model' and determine which control measure(s) failed – or indeed whether the contributors had not previously been considered in the safety analysis (in which case the Operator would ensure analysis was undertaken to correct the omission).

Once the failed control(s) has been identified then these (weighting factors/probabilities) can be amended in the FTA/ETA to show the updated Accident Risk and its effect on the overall Aircraft Total Risk. This will provide ammunition to strengthen the failed controls.

The *SATURN SAFETY MODEL* in Figure 55 depicts the high-level generic sequence from the causal factor (pitot tube i.e. sensor failure) to the accident Loss of Control. The breakdown of this model in APPENDIX 3 – Case Study for '*SATURN SAFETY MODEL'* (Air France Flight 447 Disaster) shows the failures as:

- Design Control: Redundant sensors – the 3 pitot tubes were the same and therefore were subject to common mode failures

- Key (Platform) Hazard procedural control failure – operating procedure to control the aircraft for '*Unreliable Indicated Airspeed* (IAS)' (at 5 degrees nose up and 85 per cent power is the standard procedure);
  [Although having identified and called out the loss of the speed indications, neither of the two co-pilots called the procedure "Unreliable IAS"] [92]
- Emergency recovery procedures (and training) – once passed the hazardous state of undetected speed error the pilot should have recovered the aircraft before the onset of stall i.e. the warnings of stall normally include 'stick-shakers' and warning horns; *neither of the pilots formally identified the stall situation* [92]. Had they done so (and had the appropriate training) they would have pushed the nose of the aircraft down to regain airspeed and hence lift over the wings. The author (previously a Flight [Air] Engineer) has practised stall procedures as part of flight crew drills both in normal training and in recurrent simulator training on the VC10 aircraft. Additionally crews were trained on 'wind-shear' approaches and this involved 'riding' the stall warning systems with full power. This sort of training was not conducted by the two co-pilots according to the BEA report [93].
- No Limitations in place either to;
  - Avoid the altitude that the pitot-tubes could be subject to super-cooled water droplets and icing i.e. fly below Flight Level 310 (this would require more fuel to be carried to cross the Atlantic)
  - Avoid Flight in Icing conditions and flight in or near thunderstorms i.e. fly around (divert off track) any Cumulonimbus clouds (this would require more fuel to be carried if the forecast indicated clouds)

Any of these design or operator controls could have broken the accident chain (as described in 2.2.9 'Safety Culture') and hence this was a totally avoidable accident.

In terms of a joint DO-Operator analysis the following Waterfall diagram should have been used to identify the new safety risk (to the operator) and then analysis should have been identified with the risk reducing (from each control) until eventual risk elimination by design.

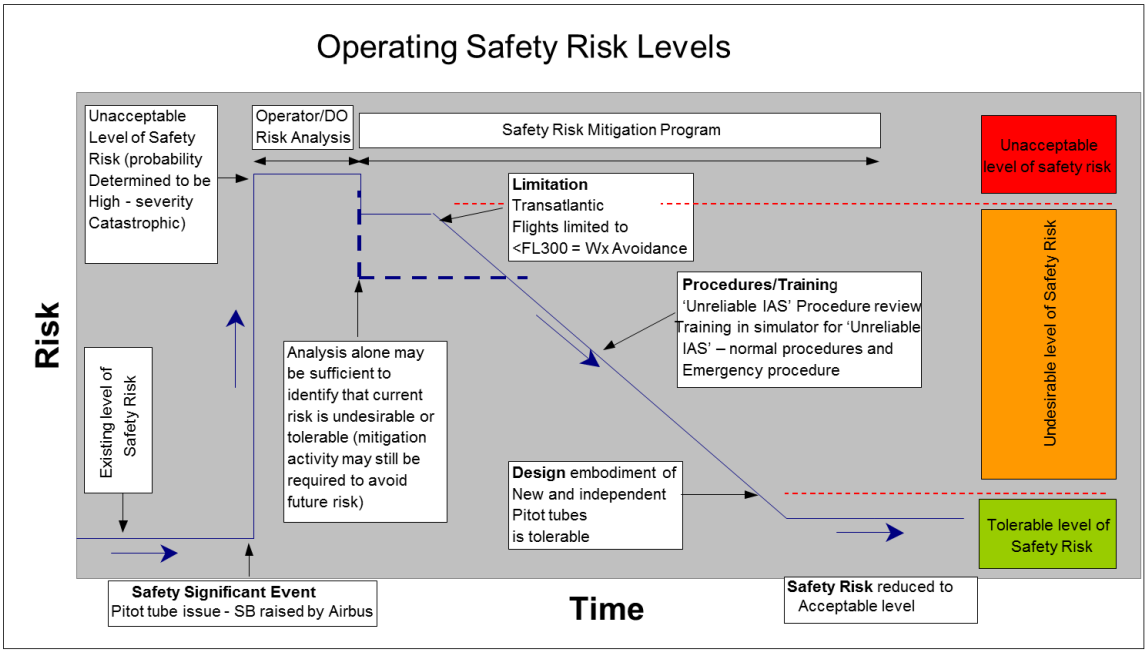


Figure 57: Safety Risk diagram for the Air France AF447 Scenario

The BEA Interim Report No.3 states that Air France has introduced the operator control measures in terms of briefing, training (in simulators) and revised the *Unreliable IAS* procedures. Also the design

measures required of the SB have been implemented and so the Safety Risk is now down to a Tolerable level of risk per the diagram in Figure 57.

3.4.7.2 Case Study Summary – Space Shuttles Challenger & Columbia

The rationale for also including the Space Shuttle disasters is twofold; firstly they represent the space community and secondly because of the closeness of the Design Authority and the Operator (namely NASA – they contract for the Space Shuttles to be built and then they Operate them). This case study summary will focus on the common themes of the two accidents within the framework of the *SATURN SAFETY MODEL*.

Both the Challenger & Columbia disasters were essentially avoidable due to the common mode of managerial failure (Risk Normalisation). As NASA are responsible for both ends of the mitigation scale (design barrier controls and operator recovery controls) there is no excuse for not managing the hazards and Risks correctly.

Investigation by Dr Richard Feynman [8] detailed that:

- Unreliability of O-Ring seal was well known
- NASA had data on 'blowbys'
- On eve of the launch engineers at the suppliers stated that the launch should NOT go ahead at temperatures below 53°F
- NASA challenged the advice and the engineer supplier management backed down
- The Launch occurred early on the morning of 28 Jan 1986 with the seal temperature at 29°F
- The management decision led to the accident probably based on 'Risk Normalisation'

This can be translated into the following categories:

- Known Issues
  - O-Ring issues on previous spaceflights (Challenger)
  - Foam Tiles had previous detached (Columbia)
  - Engineering concerns raised (Cost versus Safety?) (Challenger & Columbia)
- Complacency
  - NASA safety culture was deemed 'lamentable' by Diane Vaughan [7] (for Challenger, but there was still no improvement some 17 years later for Columbia)
- Lack of (Safety) Risk Management
  - No mitigation
  - Procedure – the Flight Readiness Review is the final 'managerial' process and this is where the 'cost versus safety versus late scheduling' was an issue for NASA; this is where the link in the accident chain can and should have been broken (Challenger & Columbia)
  - Procedure for a damaged Space Shuttle in Space – was there one? There may be a scenario (such as the fatal Columbia sortie) whereby the vehicle is deemed unrecoverable (at that moment) and therefore the 'Plan B' procedure should be to keep the astronauts on the ISS until a rescue Launch can be made. In the meantime the astronauts can take extensive pictures (which they did) to aid in the decision on repairing the damage (or not). Arguably if the decision was that the vehicle was not repairable then there should have been two further options;
    - Leave it attached to the ISS for training and spares purposes
    - Controlled destruction of the vehicle by re-entry into the ocean or by sending it into 'deep space'/towards the sun, etc.

In a sobering reality, the decision of all of the above could have been made on a cost (of losing the vehicle i.e. leaving it in space) versus the benefit concerning the cost of the 7 astronaut's lives for Columbia; however this is merely a thought and no evidence points to this. In the military and in spaceflight the flight crew know the risks and know that they may die but clearly all is done that is reasonably possible to provide safe vehicles.

The *SATURN SAFETY MODEL* in Figure 55 depicts the high-level generic sequence from the causal factor (i.e. o-ring failure) to the accident Loss of Control. The breakdown of this model in APPENDIX 4 – Case Study for '*SATURN SAFETY MODEL'* (Space Shuttle Challenger & Columbia Disasters) shows the failures as:

Space Shuttle Challenger;

- Pressure sensors not providing sufficient data in time
- Flight Termination System – not able to protect the astronauts in time
- Crew Pod ejection – not able to protect the astronauts in time
- Limitation ignored – the 53° F limitation for the O-Rings were ignored by the management against the engineer's advice

Space Shuttle Columbia;

- Cause Control failure – Lack of Quality Assurance to check the adhesive properties of the heat resistant foam tiles
- Lack of Space Shuttle repair policy whilst docked at the ISS (leading to decision to return Columbia without repair)
- Crew Pod ejection – low survivability; as the airframe started to break up the crew should have been able to eject the crew pod safely and float the Earth. This facility was not properly thought out

3.4.7.3 Summary of Space Shuttle Disasters

Both Space Shuttles and crew were lost due to a catalogue of errors involving **m**anagement and as a result of NASA's *lamentable* safety culture. It is clear that for the orbital space operations the various levels of controls should be explicitly detailed within accident sequences and these controls should be examined and managed more thoroughly (than say their aviation counterparts) due to the exacting environment and fantastic momentum that the Shuttles endure. This was not done effectively in both of these accidents and arguably considering the Heimlich Ratio (Figure 5) and Space-related accidents and serious incidents (Table 3) then it would appear that the poor accident rate could have been a lot worse.

These space-related case studies (and the Air France AF447 case study) should be stark reminders to the nascent suborbital domain to manage their operations effectively from the onset and in particular to have a contiguous and explicit safety model from which to understand their accident risks and from which to effectively and proactively manage their controls.

3.4.8 Exemplar Safety Model – The Hazard and Safety Risk Management Log

As a result of the introduction of a Safety Model a prototype Hazard Log has been developed that accommodates the methodology of the Safety Model. As opposed to Design Organisation hazard logs and separate Operator Safety Risk management tools (risk profiles and hazard logs), the *Saturn SMART* Hazard Log provides an integrated approach that is User-friendly and provides relevant information and reports to enable Duty-Holders to make appropriate Safety-related decisions; mainly concerning Risk but also concerning design changes.

In designing the *Saturn SMART* hazard log it was important to start with ICAO User Requirements as detailed in Section 2.2.7:

- *Record hazards*
- *Have hazards with unique assigned numbers*
- *Describe each hazard*
- *Detail the consequences*
- *Assess the likelihood and severity of the Safety Risks*
- *Detail safety risk controls (mitigation measures)*
- *Be updated for new hazards and safety risk controls*

Additional Identified Requirements for the Integrated Safety Model are as follows:

- Tool must be capable of recording relationships and associations between Accidents, Hazards (Key (Platform) Hazards, System Hazards i.e. failure conditions and Inherent Hazards), Causes and Controls
- In addition the tool must be able to cope with differing layers of hazards i.e. a lower-level system hazard, a Failure Condition and a Key (Platform) Hazard (as well as Inherent hazards)
- Tool must be capable of recording probability/frequency values as attributes of these entities (including pre- and post-control values for Accidents and Hazards)
- Tool must be able to assign severity values to Accidents
- Tool must be able to display Accident Risk classifications
- Tool must be capable of recording Air Safety Reports and displaying in standard Risk Profile format
- Tool must be User-Friendly; this means ease of Navigation between screens, visually representation of the hazard-accident relationships and visual and logic numbering scheme
- Tools must have a search function for ease of use

In simplistic terms the architecture for the relationships (between cause, hazard, accidents and controls) required a 'Many-to-Many' tabular scheme in order to accommodate the requirements. Figure 58 below depicts the construct of the database in terms of relationships:

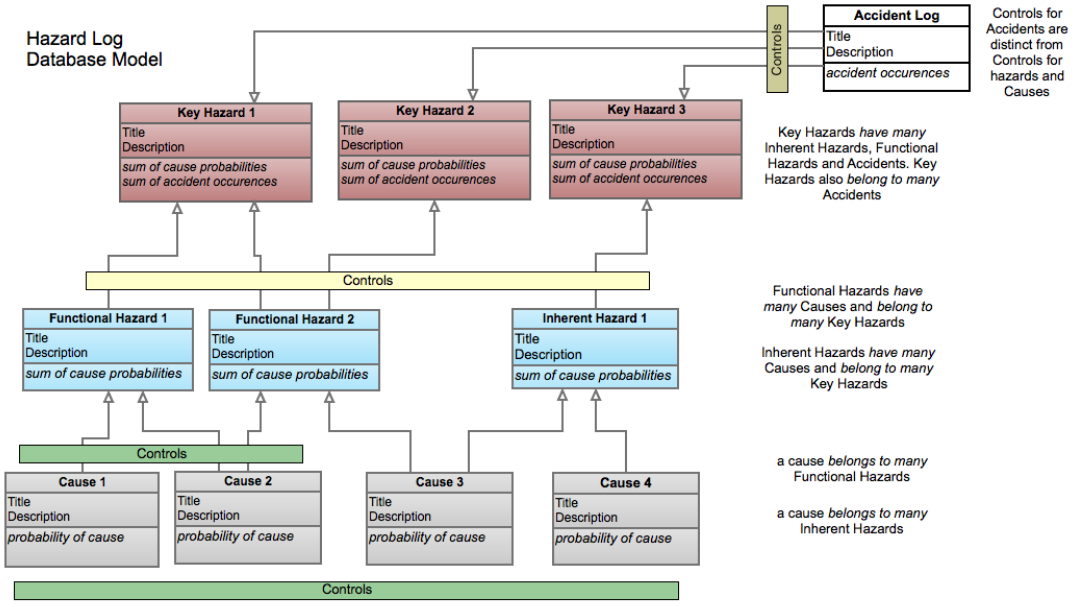


Figure 58: *Saturn SMART* Hazard Log Construct

Thereafter the tool was developed to have layered user-friendly screens to enable a clear and visual representation of the hazard-accident sequence and to enable the user to be able to navigate to the different levels by use of a logical numbering scheme and easy to follow steps.

The purpose of the tools is to demonstrate that the contiguous safety approach can be managed i.e. within a safety tool. Figure 59 shows an early version of the 'working area':

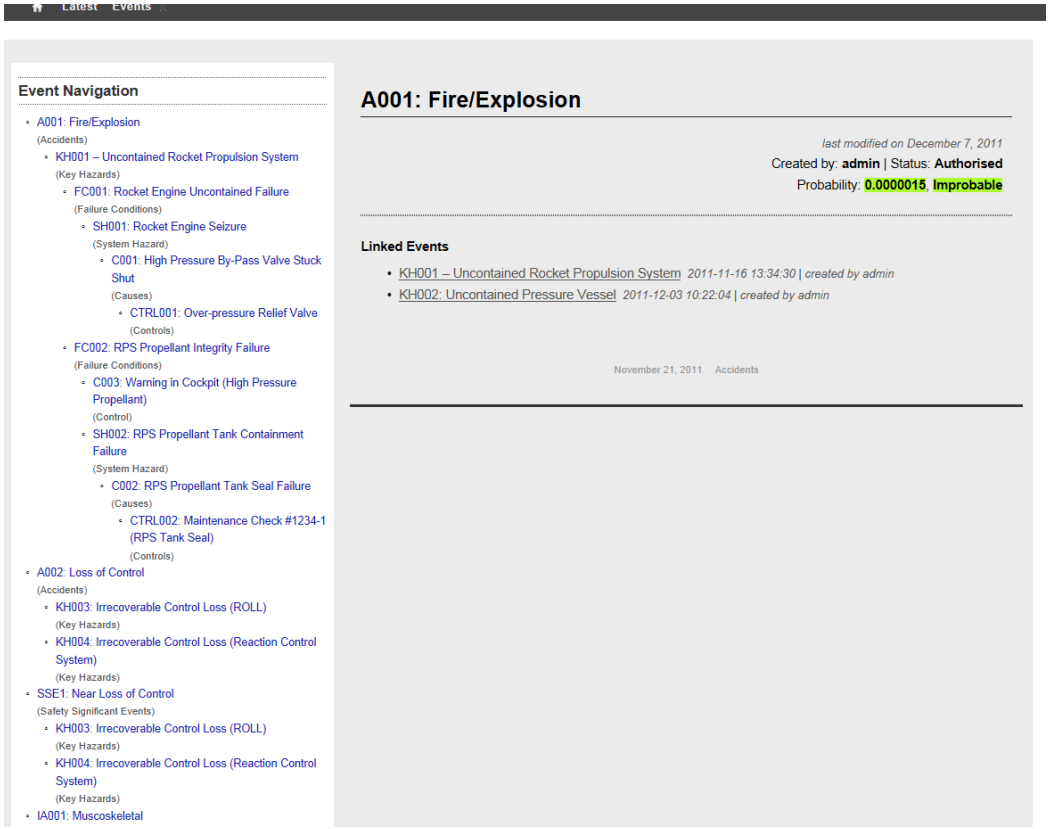


Figure 59: Saturn SMART Hazard Log development

3.4.9 Exemplar Safety Model – Applying ALARP

The review of the ALARP principle in Chapter 2.2.6.3 highlighted that there was confusion in terms of applying the ALARP principle (based on workplace risks and measured in risk of death per person per year) with an aircraft's airworthiness and safety risks. This section aims to clarify the differences and provide an example (for the inherent people-based risk reduction) to help illustrate the ALARP process as applied to a space-related vehicle (SoA) or indeed an aircraft.

Functional & Operator-based Risk Reduction

It is considered that the DOs are familiar with and should continue with the fail safe design philosophy and employing the safety precedence sequence to reduce the likelihood of an event and in order to meet safety objectives. Here they are applying mitigation in order to reduce the risk of an accident happening but actually they are ultimately reducing the probability of a failure condition (and where possible reducing the severity by eliminating a hazard or introducing a safety feature such as a physical barrier that may limit the propagation of a hazardous state).

It is considered that the *SATURN SAFETY MODEL* should be followed and that Operators follow through with the contiguous safety effort in terms of managing the risks at the Accident Level. To do this Operator's aim is to reduce the risks by the implementation of operating procedures, training and

Limitations. Their focus is on operating occurrences and ensuring that the controls (or failures thereof) are analysed sufficiently and also to ensure the occurrences are fed back to the DO in order that the DO can update the base events within their fault trees. Should events occur that lead to a required design change as the mitigation then it is here that the ALARP principle could be employed. The Cost Benefit Analysis technique then explicitly shows as part of the optimisation analysis whether the cost of implementing the change (risk reduction) is grossly disproportionate to the benefit gained. This can be calculated in terms of flying hours initially to obtain an 'ALARP Budget' (see example at 4.1.2). Sensitivity analysis can then be carried out on the ALARP calculation by varying parameters such as the probability or the disproportionality value based on implementation of different control measures.

Once the analysis has been conducted and the functional-based risk reduction identified and analysed within the ALARP calculation then the operator can provide a Safety Justification statement as to why the system (including the operator procedures, etc.) is safe.

Inherent (people-based) Risk Reduction

In terms of people-based risks i.e. the 'inherent' risks, this also needs to be analysed in order to determine whether the risks are acceptable in terms of societal risks. This will allow both regulators and the individual fee-paying passengers to determine whether the risk of death per person per year is acceptable. To determine the inherent risk of death per person per year requires the flying hour airworthiness risks to be cross-referred to the exposure of certain groups (1st, 2nd and 3rd parties) to the risks involved. Figure 60 below details the proposed methodology and the following examples relate the flying hour to risk of death per person per year:

- Airline pilot: flying an airworthy aircraft that meets its safety objectives of $1x10^{-9}$ per flying hour for catastrophic failure conditions therefore meet the overall objective of $1x10^{-6}$ per flying hour for Loss of Aircraft conditions. Figure 60 shows that for an Upper Level of Tolerability (ULT) of exposure to risk of death per person per year (pppy) of 1 in 1000 then the limit on flying hours equals 1000.
- First it is important to work out the average exposure per population group i.e. for the pilots. This should take into account the total number of flying hours for the airline and the number of pilots employed.
- Currently pilots are limited to 1000 hours[24] for fatigue reasons and therefore are within an acceptable (tolerable) risk region (see figure below). To reduce the risk to pilots further, the following mitigation could be implemented;
    - Limit Pilot Flying Hours; limit pilot flying hours. In the extreme Figure 60 shows that with pilots flying only 100 hours per year than the risk has reduced buy an order of magnitude to 1 in 10,000 pppy. However this would not be practical and so managers should apply a reasoned and pragmatic approach in managing the exposure of risk to their pilots. At least by being aware of the issue and showing by use of Figure 60 that if a limit of 500 flying hours was imposed that their exposure to risk would be reduced fivefold to 1 in 5000 risk of death pppy.
    - Simulator Training; by limiting flying hours managers should increase the simulator training hours so that pilots can keep current. This will have an additional benefit in the pilots skills will increase thereby adding to the safety effort – this may have averted the Air France Flight 447 disaster in that the

[24] http://www.risingup.com/fars/info/part121-503-FAR.shtml

crew would have recognised the issue and acted earlier and with the correct actions.

- Suborbital Aircraft Pilot; here is a chance to better understand the exposure to risk to SoA pilots. Let us assume that the joint approach in 3.4.10 is used and we have a catastrophic risk as $1x10^{-5}$ per flying hour;
  - Flying Hours; here we can clearly see that an SoA pilot should be limited to 100 hours per year
- Spaceflight Participant: An SFP whom flies once a year is clearly exposed to the risks far less than the pilot. The risk of a catastrophic event is 1 in 100,000 per person per year and is within the tolerable risk band; the risk of a single death is 1 in 10,000. Should the target not be as stringent (or set as a requirement) and an operator has a launch license in the US then they are required to provide the SFPs with all necessary information to enable the SFPs to assess the risk such that they can then sign a waiver. In this instance should the evidence show (using Fault Tree Analysis) that the cumulative catastrophic risk is nit $1x10^{-5}$ per flying hour and is $1x10^{-4}$ per flying hour then they can see that their risk of death is 1 in 10,000 per person per year. This therefore backs up the argument that the SFP is volunteering for an adventurous activity (as opposed to a transport service from point A to point B) and therefore accepts that the risks will be higher than that of the commercial aircraft that they flew in to the Spaceport.
  - Non-catastrophic risk; although we normally discuss catastrophic events it is more likely that we will be talking about the risk of death per person per year in suborbital flights as there are other more likely scenarios of severe injuries due to the high-g forces or non-nominal situations (including personal medical issues). Here we may apply an assumption that for every death there are 10 severe injuries and 100 minor injuries. So to calculate the risk of injuries we would start from the baseline that the catastrophic risk is $1x10^{-4}$ per flying hour then the hazardous risk is $1x10^{-3}$ pfh and major risk is $1x10^{-2}$ pfh and minor risk is $1x10^{-1}$ pfh (see operator's risk matrix at Table 19). These are the A/B boundaries i.e. the targets and the designers will be aiming to meet the 'D' (Broadly Acceptable) safety objectives in terms of their failure conditions and inherent hazards. The reality is that the designer can aim to provide assurance that they will meet the safety objectives and that their 100 arbitrary hazards will then sum to be equal to the B/C boundary (for each severity classification). Therefore it is this value that we can derive as the likelihood for informing people as to their explicit risks which equates to the following:
- Hazardous (likelihood of single death) = $1x10^{-4}$ pfh (B/C boundary) = risk of death pppy of 1 in 10,000 with 1 hour flight per person
- Major (likelihood of severe injury) = $1x10^{-3}$ pfh (B/C boundary) = risk of severe injury pppy of 1 in 1,000 with 1 hour flight per person
- Minor (likelihood of minor injury) = $1x10^{-2}$ pfh (B/C boundary) = risk of minor injury pppy of 1 in 100 with 1 hour flight per person

Looking at this in perspective it appears reasonable to assume that 1 in 100 people will receive minor injuries due to g-force related or non-nominal-related events (based on an average of 5 passengers per flight this would be 20 flights); this may be a combination of the vehicle and flight profile but will clearly be related to each individual's medical condition i.e. ability to cope on such flights. This is why the medical and training criterion is so important (as mitigation to specific inherent hazards like excessive 'g-force').

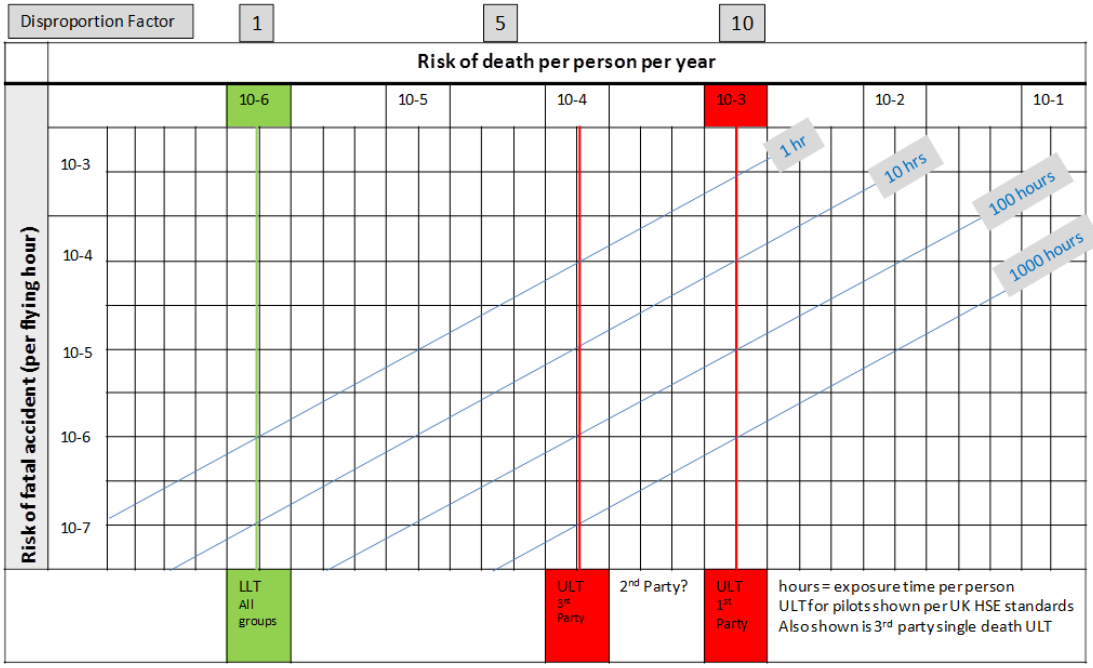


Figure 60: Exemplar Functional-based to People-based conversion of Risk values

It is considered that further analysis should be undertaken to better understand the operating and support risks that the various groups will be exposed to i.e. pilots, spaceflight participants, support personnel and third parties. This will require OHHA and OSHA activities to be undertaken and also to provide approximate numbers of people per group i.e. 10 pilots per Operator, 6 spaceflight participants per flight (with only one flight per year per SFP assumed) and 20 support personnel (directly involved in the support activities on or around the aircraft). The OHHA and OSHA activities will detail functional and inherent hazards that can cause harm to the different groups in terms of:

- Hazardous classification (single death $1^{st}/2^{nd}$ parties per Table 15):
- Major classification (severe injuries $1^{st}/2^{nd}$ parties per Table 15):
- Minor classification (minor injuries $1^{st}/2^{nd}$ parties per Table 15):
- Negligible classification (inconvenience and requires assistance and is reportable for 2^{nd} parties only per Table 15):

As can be seen above Operators may have relatively high risk concerns with these OHHA-OSHA type hazards and these need to be identified in the first instance and then managed to ALARP (or similar) in the second instance. Additionally due to the potential for high risks in operating and support SoAs these categories need to be considered within the Total System's Risk as detailed in 3.4.11 below.

3.4.10 Safety Target

The *SATURN SAFETY MODEL* takes cognisance of the Safety Target combined with safety objectives methodology that would suit a new integrated safety approach. Currently in the aviation domain the safety objective approach is used for the DOs and Operators tend to have safety goals/objective in terms of Risk Profiles (to reduce the number of events and in particular SSEs). A Safety Target approach alone focuses on the key risks rather than the airworthiness codes and this limits the use of this approach to the issue of restricted certificates and permits to fly.

The Safety Target combined with safety objectives by airworthiness codes is important within the SoA domain in order to provide a flexible but robust method of demonstrating compliance for certification. This is even more important due to the failure rate associated with the Rocket Propulsion

System; a rocket may achieve $1x10^{-4}$ per fling hour at best ($1x10^{-6}$ when combined with exposure factors possibly) and therefore would fail to meet catastrophic safety objectives. Within a safety target approach although this would take up a large portion of the safety budget then this drives the designer to design the rest of the system to meet the safety objectives ($1x10^{-7}$ per flying hour for instance) in order to meet the safety target.

3.4.11 Total System Risk – Total Risk Per Severity Classification

Aircraft Design Organisations are only interested in meeting failure condition safety objectives in order to get their aircraft certified as 'airworthy'; though they must clearly demonstrate compliance to the requirements for Continued Airworthiness. As they do not primarily concern themselves with the Operator Safety Risk Management aspects, they assume that because the safety objectives have been met then the overall System must be safe.

Now that the DO analysis is complete and the Operator has constructed Accident (& Incident) sequences, the Operators will be able to estimate and evaluate the single Accident/Incident Risks (r) effectively (for instance using the Accident Risk Matrix at Table 19) and also undertake Risk Reduction activities. These Accident/Incident Risks (r) are derived from undertaking the standard functional hazard analysis and linking these to the Accidents in Table 12 and Table 13. Additionally the Inherent-based analysis (OHHA and OSHA) must be linked to appropriate Inherent-based Accidents.

Once all of the identified single (Accident/Incident) Risks (r) have been accepted, their cumulative probabilities will be known i.e. the sum of contributing hazards (failure conditions and inherent hazards) equates to the Accident/Incident's probability. The single (Accident/Incident) Risks (r) could then be summed to determine the Total Risk per Severity Classification (R_S) and then the Total System Risk (R) could be calculated for the platform.

However great care must be applied when undertaking this task as the different Accidents and Incidents will have different severity classifications; these will require a 'weighting' scheme to be applied (typically 10, 1, 0.1 and 0.01). After summing the Severity Risks (R_S) in each severity column one could then see the level of Risk (R) by joining the cumulative points by drawing a line. This approach is akin to the 'iso-risk' lines in Figure 61 below.

The relationships of the individual accident risks (r), the Total Risk per Severity Classification (R_S) and the Total Risk (R) can be presented thus:

$$\mathbf{R = R_S\,(_{catastrophic}) + R_S\,(_{hazardous}) + R_S\,(_{major}) + R_S\,(_{minor}) + R_S\,(_{negligible})}\ \textbf{[}\textit{Equation 4}\textbf{]}$$

Where $R_S = r_{(n1)} + r_{(n2)} + r_{(n3)} \ldots..$

By having a Risk Matrix, the Operator will be able to determine:

- Whether the DO's failure conditions meet their respective safety objectives
- Where each 'single Risk' (r) (Accident/Incident) is classified. Where Risks are 'B' or 'C' class Risks the Operator will be able to determine which failure condition(s) is the main contributor in order to undertake Risk Reduction to ALARP
- What the total risk per severity classification is (R_S); this is important when a catastrophic safety target is to be met for instance
- What the cumulative 'Total System Risk' (R) is and whether it meets the determined Total Safety Target.

So what is the Tolerable Level of Safety (Equivalent Level of Safety) for a commercial spacecraft? What Safety Target can we set for the whole platform(s)? It is considered that this is the only real problematic area for further consideration. At present, Total System Risk Target is not considered by Design Organisations or Operators in the aviation industry and there is no guidance on achieving this. One such method could employ the use of 'iso-risk' lines as suggested by Tech American Standards [84]. Their scheme dictates that to measure the total system risk (R), one needs to provide a measure of severity (in terms of fatalities) and a measure of probability of the occurrence. The 'measures' of total system risk (R), include:

- *Expected Loss Rate*
- *Maximum Loss Rate*
- *Most Probable Loss Rate*
- *Conditional Loss Rate*

In relation to 'Conditional Loss Rate' the sum of the probabilities for all hazards is considered (with the assumption of independence) and this could be most appropriate.

Understanding the Total System Risk (R) is even more important within an emerging and novel industry where immature technology is yet to be rigorously proved; but first a Target (ELOS) must be set.

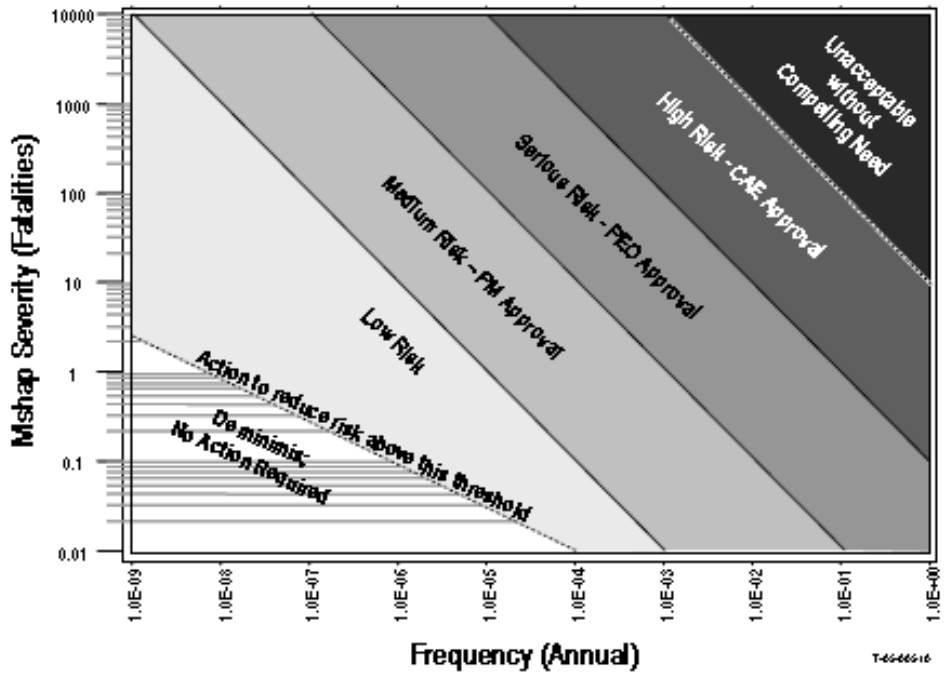


Figure 61: Tech America Standard exemplar Total System Risk Assessment Criteria incorporating 'Iso-Risk' lines

Arguably DOs will undertake a combined test and evaluation process (with Operators) but this will still not provide sufficient quantitative evidence of failure condition probabilities in some cases; instead qualitative engineering judgment may be used and hence the 'confidence' level of this type of analysis will need to be clearly stated. Thus, Operators in the United States will need to take the DO's analysis (that may have met safety objectives that do not have the standard high confidence levels per aviation) and apply their Safety Risk Management efforts as described above. This approach is considered necessary in order to fully understand the Risk presented by the whole platform(s). In Europe however, a different approach will be taken; one which is based on known certification

processes. This will be to a predetermined safety target (for catastrophic loss) and therefore it will be important to derive the cumulative risks per severity classification (R_S).

3.4.12 To Launch or Not to Launch

The Challenger disaster in 1996 provides a good example whereby a Flight Readiness Review (FRR) system was in place at NASA but the **M**anagement's (in the 5-M model at Figure 22) decision to launch over-ruled the engineering advice not to launch due to the temperature limits of the 'O-ring' seals; the Space Shuttle launched with temperatures of 29°F, whereas the design specifications were 53°F.

The FRR is a good method to providing a 'Go/No-Go' decision regarding a launch of a suborbital aircraft and it is essential that key stakeholders are represented at the FRR and decisions recorded such that the **Accountable** person and **R**esponsible person(s) (within the RACI chart at Table 22) formally agree on the decision. The following chart presents an exemplar SoA FRR Flight Risk Assessment (FRA). The current chart is split into two segments; the flight/environment segment and the human factors segment. The rationale is to represent the 5-M model's path to **m**ission success rather than **m**ishap.

The events chosen were from the author's knowledge of flight operations and the suborbital domain and include:

- Flight Plan/ATM
- Flight Profile
- Weather conditions
- SoA status in terms of Limitations and Deferred Faults
- Carrier aircraft (if applicable) status in terms of Limitations and Deferred Faults
- Flight Crew
  - Qualification/Currency
  - Simulator Currency
  - Human Factor#1 – Fatigue/Complacency
- Passengers
  - Human Factor#2 – interaction in flight

These are basic issues that could have an impact on a flight and there will clearly be more.

Recommendation: It is recommended that the IAASS SSS TC undertake analysis based on the findings in 3.4.12 in relation to Flight Readiness Review (FRR) Flight Risk Assessments. These recommendations are collated at 6.4.8.

FLIGHT FACTORS				
		Flight Plan Changes		
		No Changes	Few Changes	Big Changes
Flight Plan/ ATM Integration	Test Pilot	**1**	**2**	**3**
	Experienced Pilot	**2**	**3**	**5**
	Mix – Test Pilot or Experienced + Training Pilot	**3**	**4**	**6**
		Complexity		
		Routine	Standard	Complex
Flight Profile	Standard profile	**2**	**3**	**4**
	Extreme Apogee profile	**3**	**4**	**6**
	Other profile	**5**	**6**	**8**
		Forecast Weather		
		VMC/ low wind	<3km/moderate wind	Forecast clouds/ strong wind
Take-Off Weather Conditions	Good WX Conditions	**1**	**2**	**3**
	Fair WX Conditions	**2**	**3**	**4**
	Marginal WX Conditions	**3**	**4**	**5**
		SoA Serviceability		
		Excellent	Good	Average
Suborbital Aircraft Limitation Factors	Low/Non-Critical Limitations or Modifications	**1**	**3**	**4**
	1 or 2 Major Limitations or Modifications	**2**	**3**	**7**
	Many Major Limitations or Modifications	**3**	**5**	**6**
		Carrier Aircraft Serviceability		
		Excellent	Good	Average
Carrier Aircraft Limitation Factors (if applicable)	Low/Non-Critical Limitations or Modifications	**1**	**3**	**4**
	1 or 2 Major Limitations or Modifications	**2**	**3**	**7**
	Many Major Limitations or Modifications	**3**	**5**	**6**

HUMAN FACTORS

		FLIGHT CREW CURRENCY (Last Flight)		
		<7 Days	<7 Days<30	>30 Days
FLIGHT CREW Qualification/ Currency	Test Pilot	**1**	**2**	**3**
	Experienced Pilot	**2**	**3**	**4**
	Mix – Test Pilot or Experienced + Training Pilot	**4**	**5**	**6**
		Pilot Currency (Last Simulator sortie)		
		<14 Days	>14 Days <30	>30 Days
FLIGHT CREW Simulator Currency	Test Pilot	**1**	**2**	**3**
	Experienced Pilot	**2**	**3**	**5**
	Mix – Test Pilot or Experienced + Training Pilot	**3**	**5**	**6**
		No. of Consecutive Flights in 36 hour period		
		1	2	>2
HUMAN FACTOR #1 – Flight Crew (fatigue/ complacency)	Test Pilot	**1**	**2**	**3**
	Experienced Pilot	**2**	**3**	**4**
	Mix – Test Pilot or Experienced + Training Pilot	**3**	**4**	**5**
	Experienced Pilot	**2**	**3**	**5**
	Mix – Test Pilot or Experienced + Training Pilot	**3**	**5**	**7**
		Number on Board 'v' fitness level		
		>4	>2 but >4	<2
HUMAN FACTOR #2 – Space Flight Participant	Fitness level (factor of fitness/age/ability to cope as determined by Chief Medical Officer)	**2**	**4**	**6**
FLIGHT RISK	**LOW**	**MED-LOW**	**MED-HIGH**	**HIGH**
Score	**10-20**	**20-30**	**30-40**	**>40**
Classification	Risk is low and no flight issues present – GO	The flight involves some concern that needs discussion as to the acceptability – GO once agreed	The flight involves complex issues that need to be individually discussed before a GO decision is made. Formal Authority required from Accountable person (CEO)	STOP. The flight involves very high risks and these must be addressed to determine whether the flight should continue. In some cases a further Limitation may be required in order to achieve a 'GO' status – this must be formally agreed by the Manager (CEO)

Table 22: Exemplar FRR – Flight Risk Assessment

3.5. SPACEPORT SYNTHESIS

3.5.1 Introducing Spaceports

What is a Spaceport? According to Wikipedia[25] a spaceport is:

> *A spaceport or cosmodrome (Russian: космодром) is a site for launching (or receiving) spacecraft, by analogy with seaport for ships or airport for aircraft. The word spaceport, and even more so cosmodrome, has traditionally been used for sites capable of launching spacecraft into orbit around Earth or on interplanetary trajectories. However, rocket launch sites for purely suborbital flights are sometimes called spaceports. In recent years new and proposed sites for suborbital human flights have commonly been named spaceports.*

'Spaceports' are emerging all over the world in an attempt to lure SoA/RLV Operators to commence operations in their area and thereby attracting 'space tourism' and boosting their economies. Examples include 'Spaceport Scotland'[26] and 'Spaceport Sweden'[27] who aim to lure Virgin Galactic to operate from their area. The issue for both of these opportunists and many more is that the necessary safety and environmental regulatory requirements are not in place.

3.5.2 Identifying Spaceport Requirements

In some cases spaceports are already in operation as airports and this is the case for the two cited above; Spaceport Scotland is currently Royal Air Force Lossiemouth and Spaceport Sweden is currently Kiruna Airport. In the United States there are many existing orbital spaceports and some of these may attract the SoA/RLV operators with the cancellation of the Space Shuttle Program. In these cases whereby existing infrastructure and operating rules are in place then the spaceport authorities will need to identify the delta requirements to be able to operate as a spaceport.

However where new runways are being built as a spaceport, they may arguably qualify as being an airport.

In both cases, existing or new-build, regulatory requirements must be considered in the first instance. In terms of regulations or guidelines the FAA-AST have only provided environmental guidelines and consequently have only undertaken environmental assessments (EAs - see 3.5.3 below). There are no spaceport safety requirements from EASA as yet and the FAA-AST safety-related aspects are not separate and explicit as they are detailed within the general Launch Site License regulations of CFR 420 [96].

Additional issues to be resolved for those European and other non-US spaceports wanting to obtain business from Virgin Galactic (and other US-designed vehicles) is that the US 'export controls' (on technology) will currently impact the ability to do so. This aspect is still to be worked out by the spaceports, operators and regulators.

The approach taken for this Section is to review the EAs and determine whether any correlation to safety can be derived. Then relevant safety requirements shall be reviewed within the CFR 420. Additionally a review of existing airport safety requirements will provide further discussion.

---

[25] http://en.wikipedia.org/wiki/Spaceport
[26] http://www.spaceportscotland.org/
[27] http://www.spaceportsweden.com/

3.5.3 Spaceport Environmental Requirements

Currently the FAA-AST has certified two spaceports in terms of an Environmental Assessment (EA); Blue Origin's West Texas Commercial Launch Site [93] and draft EA for Oklahoma Spaceport [94]. The EAs were conducted against the FAA-AST Environmental Guidelines [95] and examined the following environmental aspects:

- *Air Quality*
- *Airspace**
- *Biological Resources*
- *Cultural Resources*
- *Geology and Soils*
- *Hazardous Materials and hazard waste management**
- *Health and Safety**
- *Land Use*
- *Noise**
- *Socioeconomic Impacts*
- *Environmental Justice*
- *Traffic and transportation*
- *Visual and aesthetic resources*
- *Water resources*

Those aspects that correlate to safety issues will be discussed further and are annotated thus (*).

These EAs were assessed against the FAA-AST environmental guidelines [95] for obtaining a launch license permit.

Airspace: the EA details that by maintaining the vehicle within an air corridor the safety impact should be minimal:

Given the short window for need of exclusive airspace use, the infrequent launches (approximately once per week), and expected procedures for rerouting or rescheduling air traffic, the use of FAA-approved temporary restricted airspace procedures is not expected to significantly impact airspace use in the area.

The airspace requirements also concern the selection of the spaceport and also that alternative sites for the spaceport are nominated together with arguments for and against in relation to the primary and secondary locations; issues cited could be mountainous regions or the lack of emergency landing alternative.

Hazardous Materials: the EA discusses the RPS and in particular the propellants. The requirements are for robust methods of storage, transportation and handling and testing.

Propellants used for the New Shepard RLV include rocket propulsion grade kerosene (RP-1) (12,000lbs per launch) and 90 per cent concentration hydrogen peroxide (103,000lbs per launch).

The explosives are stored in a dedicated area in Department of Transport approved shipping containers. In terms of RLV replenishment the loading system would monitor propellant flow rates, pressures, temperatures and propellant load delivered.

Health & Safety: H&S issues are discussed and said to be minimal with an anticipated injury of '1' with '0.5' days lost time. Additionally the EA discusses the non-nominal situations whereby their ground personnel may be subject to occupational health hazards:

In the case where impact of the spent abort module does not result in a fire, the Emergency Response Team would wait at a safe stand-off distance until it is determined that a fire will not start (at least 60 minutes after impact).

After the fire resulting from impact has burned out or after it is determined that a fire will not start, the Emergency Response Team would don personal protective equipment (fire resistant Nomex coveralls, gloves, air packs, face shields) and approach the impact site to inspect for unburned solid propellant.

Noise: Blue Origin's RLV is a vertical rocket and hence the noise levels will be an issue. The EA states:

A low-level jet flyover could have sound approximately 100 dBA, depending on altitude and power level. Very large rocket launches such as the Space Shuttle have sound levels around 175 dBA at 50 feet from the test pad. Humans begin to experience pain at levels above 100 dBA

Blue Origin's RLV noise emissions are 85dBA at the site and only reduce to 80dBA at 8 miles. In this instance the spaceport is remotely situated and only relevant and authorised personnel will be on site and these can be provided with hearing protection. For those outside of the spaceport, blue Origin will have to provide warning signs detailing when the launches are to take place and that noise will be an issue.

Oklahoma's noise issues are represented by a variation of concept X, Y and Z RLVs. For concepts X & Z they do not anticipate any noise issues whereas for concept Y RLV (an XCOR-type of vehicle) they anticipate the noise will be similar to that of Blue Origin's above i.e. 76dBA to 86dBA.

3.5.4 Spaceport Safety Requirements

Spaceport Safety Requirements can be derived from existing airport regulatory requirements plus those derived from the EA above, from CFR 420 [96], from existing airport requirements and also from industry knowledge.

CFR 420 §420.19 details an explicit safety objective in terms of risk to the 'public' as this methodology is carried over from the standard NASA orbital flights; indeed the FAA-AAST covers orbital flights and are demanding this effort of analysis for the suborbital operators as well:

(1) A safe launch must possess a risk level estimated, in accordance with the requirements of this part, not to exceed an expected average number of 0.00003 casualties (E_c) to the collective member of the public exposed to hazards from the flight ($E_c \leq 30 \times 10^{-6}$).

As per the Air Traffic Management aspects detailed below, suborbital flights will be contained within an airspace/space corridor and the exposure to the public should be minimized by this restriction alone. Additionally the model of SoA/RLV will further dictate the likelihood of exposure to the public as follows:

- Virgin Galactic (Space Ship 2) – air drop within the safe corridor and glide to land within the safe corridor therefore public exposure none or minimal
- Blue Origin (New Shepard RLV) – vertical launch and descent in the middle of the desert within a safe corridor therefore public exposure none or minimal
- XCOR (Lynx) – this model could provide exposure to the public because the vehicle ignites its rocket on the 'runway' and the rocket phase is maintained until nearing the apogee. With this model the selection of spaceports to operate from should be limited to those in remote locations such as in a desert or mountainous regions or possibly next to the sea in a remote site i.e. well away from a City or

town.

CFR 420 §420.63 to 69 concerns the Explosive Siting aspects and details the following:

- *An explosive site plan*
- *Safe storage of rocket propellants (RP) (assumes RP-1)*
- *Safe handling of rocket propellants*
- *Issues of Solid and Liquid propellants located at same spaceport*
- *Calculated minimum separation distance (of combined propellants)*
- *Intervening barriers*
- *Crowd (public) safety within the bounds of the spaceport* – depends on the vehicle type and propellants used. The safe distance is dependent on the calculation derived from the type of explosive and amount used. In the Blue Origin case (combined total of 115,000lbs of explosive) the safe distance for a '1.3 grade' of explosive is 375ft.

CFR 420 §420.71 concerns Lightning protection at the launch site:

> *(a) A licensee shall ensure that the public is not exposed to hazards due to the initiation of explosives by lightning.*

As with 'insensitive munitions' propellants are subject to heat or ignition sources (such as lightning) and methods must be introduced to mitigate the 'extremely improbable' event. The requirements detail standard bonding and test/inspections but also include a procedural mitigation in the cases where '*no lightning protection system is required*'; this is when a '*lightning warning system is available to permit termination of operations and withdrawal of the public to public area distance prior to an electrical storm or for an explosive hazard facility containing explosives that cannot be initiated by lightning*.'

3.5.5 Spaceport Air Traffic Management Requirements

Air Traffic Management (ATM) is an essential component in assuring the safety of SoA/RLV flights. The FAA-AST has not issued guidance for the spaceport specifically however their launch license regulations and guidelines for Operators provide requirements and in particular to ATM is CFR Part 437 [97] as follows:

- FAA CFR §437.57 – *Operating Area Containment; this mainly concerns protecting the public on the ground and that the planned trajectory (orbital connotations) and non-nominal trajectory should remain within the containment area*
- FAA CFR §437.69 – *Communications (a) to maintain communications with air traffic control during all phases of flight*
- FAA CFR §437.71 – Flight Rules
  - *(b)(1) Follow flight rules that ensures compliance with §437.57 (above)*
  - *(d) A permittee may not operate a reusable suborbital rocket in areas designated in a Notice to Airmen (NOTAM) unless authorized by (1) ATC*

In terms of an operating containment area for SoA/RLVs Dan Murray's[28] paper on Air Traffic considerations for future spaceports highlights the issue of protecting the public and also protecting other aircraft should the SoA/RLV 'explode'; he cites the concern of a one pound fragment of steel (from an exploding vehicle) having the potential to puncture the body of an aircraft flying below and further cites the Space Shuttle Columbia accident as evidence. His paper looks at the possibility of

[28] Dan Murray is one of the FAA-AST specialists

introducing ‘corridors’ either between airways (in high-density flight areas) or even across airways; both of these would require NOTAMs and possible use of the corridors at off-peak times or days i.e. he suggests air traffic is considered lighter on a Wednesday or Saturday and before 10am as opposed to a Monday or Friday.

3.5.6 Aviation Airport Requirements

Airports are required to be certified and the FAA has CFR Part 139 [99]. As detailed at the start of this Section some emerging spaceports are currently airports and these will already have certification to operate. The airport certification requirements cover:

- *139.301 Records.*
- *139.303 Personnel.*
- *139.305 Paved areas.*
- *139.307 Unpaved areas.*
- *139.309 Safety areas.*
- *139.311 Marking, signs, and lighting.*
- *139.313 Snow and ice control.*
- *139.315 Aircraft rescue and fire-fighting: Index determination.*
- *139.317 Aircraft rescue and fire-fighting: Equipment and agents.*
- *139.319 Aircraft rescue and fire-fighting: Operational requirements.*
- *139.321 Handling and storing of hazardous substances and materials.*
- *139.323 Traffic and wind direction indicators.*
- *139.325 Airport emergency plan.*
- *139.327 Self-inspection program.*
- *139.329 Pedestrians and Ground Vehicles.*
- *139.331 Obstructions.*
- *139.333 Protection of NAVAIDS.*
- *139.335 Public protection.*
- *139.337 Wildlife hazard management.*
- *139.339 Airport condition reporting.*
- *139.341 Identifying, marking, and lighting construction and other unserviceable areas.*
- *139.343 Noncomplying conditions.*

Additionally to the requirements above the FAA introduced AC 150/5200-37 [26] which details guidance for an SMS for Airport Operators. The Safety Risk Management provides useful guidance for airport hazard identification:

- *The equipment (example: construction equipment on a movement surface)*
- *Operating environment (example: cold, night, low visibility)*
- *Human element (example: shift work)*
- *Operational procedures (example: staffing levels)*
- *Maintenance procedures (example: nightly movement area inspections by airport electricians)*
- *External services (example: ramp traffic by Fixed-Base Operator (FBO) or law enforcement vehicles)*

CAP 642 also provides useful ‘Airside Safety Management’ principles and details common hazards as:

- *Vehicles striking aircraft and/or people*
- *Hazards to passengers on the apron*
- *Moving aircraft (including aircraft on pushback or being towed)*

- *Live aircraft engines (including helicopters)*
- *Falls and falling objects*
- *Operation of air-bridges*
- *Manual handling*
- *Noise*
- *Work equipment (including machinery)*
- *Hazardous substances and Dangerous Goods (including radioactive substances)*
- *Inadequate lighting, glare or confusing lights*
- *Adverse weather conditions (including winter operations)*
- *Slips and trips*
- *Electrical hazards*
- *Faults and defects*

Derived Spaceport Safety Requirements - ATM

The above requirements for Operators can then be turned into requirements for Spaceport Air Traffic Management:

(a) Flight Planning: the Spaceport, on receipt of a notified suborbital flight plan, must;

- Issue a NOTAM of the intended suborbital flight. The NOTAM will provide sufficient mitigation to exclude other air vehicles. This must be for a 'corridor' of specified altitude, length and width
- Ensure standard integration and separation with aviation traffic when not in the 'corridor'
- Ensure the maximum altitude of the NOTAM is no greater than 150km (above this altitude the NOTAM is no longer valid and the Operator must seek orbital collision avoidance analysis)
- The Spaceport authority should also ensure that the NOTAM area has minimal (or none) populated areas i.e. over the desert, inhabitable mountains or over the sea
- The Spaceport authority should provide 'windows of opportunity' for SoA/RLV Operators whereby the air traffic is 'light' within or near the corridor; this can reduce the exposure of other air traffic thereby reducing the exposure to a mid-air collision

- Flight Rules; the SoA/RLV should remain within visual flight rule (VFR) conditions at all times unless the vehicle is certified for Instrument Flight Rules (IFR)
- Communications: the Spaceport must be able to remain on contact with the SoA/RLV by;
  - Radio communications (mandated for the SoA/RLV)
  - Data communications
    - IFF (mandated for the SoA/RLV)
    - Tracking (desirable for the SoA/RLV) – includes real-time position and velocity

Spaceport Safety Management System

An existing airport should have an SMS in place and be compliant to standards however in the case of a new Spaceport or an airport evolving to be a Spaceport should ensure that an effective SMS is implemented. This is particularly important in the development of a new Spaceport with the

opportunity to build a safety culture with the right ethos from the beginning. This will require an effective and robust Safety Management Plan to get all stakeholders on board.

Safety Management Plan

The Spaceport Authority should provide a Safety Management Plan as the overarching document to which organisations such as ATM, SoA/RLV Operators and supporting entities are to be compliant with. This is an opportunity to provide a useful tool and effective structure in which to orchestrate the combined safety effort for the different organisations that will form the Spaceport Safety Panel. The SMP will detail the safety criteria safety requirements for all to follow. Additionally the SMP should provide a RACI chart (detailing who is **r**esponsible **a**ccountable, **c**onsulted and **i**nformed) in terms of safety because otherwise one organisation may think that the Spaceport Authorities are responsible when in actual fact the SoA operator is responsible for instance. The SMP will also cover the Emergency Response Plan & Major Incident Plan as Annexes.

Spaceport Safety Case(s)

The Safety Management System should comprise explicit safety cases for Spaceports due to the additional hazards and issues highlight in the sections above. The following guidelines are proposed:

- Spaceport Safety Case: this is the overarching safety case that provides a robust argument supported by evidence that the Spaceport is acceptably safe. This is supported by the following sub-tier safety cases/goals:
  - Spaceport Safety Management; this is one leg of the safety argument and is the Spaceport SMS. Here the argument should describe the following;
    - Spaceport Safety Organisation (and Safety Panel) with representatives from;
      - Spaceport Safety Manager
      - ATM Safety Representative
      - Operator Safety Manager(s)
      - Maintenance Safety Representative
      - Supporting Activity Representatives (as required)
    - Spaceport Safety Policies
    - Spaceport Safety Targets and Safety Requirements
  - ATM Safety Case; the Air Traffic domain are already well versed in safety management and working to safety requirements, objectives and targets. This will need to have additional work to address the changes enforced by operating SoA/RLVs. Specific areas to address will be;
    - Flight Planning
    - Flight Operations
    - Communications safety case
  - Maintenance Safety Case
- Support Activities Safety Case
  - Explosives Safety Case
    - Storage
    - Handling
    - Transportation
  - Customer (SoA/RLV Operator) Safety Case: the Spaceport Authorities need to provide a leading role in the safety of the Spaceport as far as Operators go

3.5.7 Hazard & Risk Management

In terms of hazard and risk management the Spaceport Safety Case will have to derive safety targets and safety objectives for the following:

- Spaceport Functional Safety – Air Traffic Equipment; the ATM Safety Case will conform to existing requirements for commercial aviation. This details a safety objective approach i.e. $1x10^{-9}$ per flying hour for failure of equipment and then also considers the ATC operator human factors. The addition of managing SoA/RLVs will need to be factored in to the SMS; a subcomponent of SMS is 'Change Management' and integrating SoA/RLVs will provide challenges and additional safety requirements as detailed above i.e. the establishment of an air corridor. These changes should be able fit within the existing ARM framework.

- Spaceport Inherent Safety; This aspect will cover the operating and support activities (OSHA) and occupational health activities (OHHA) concerned with the existing airport (if applicable) and integrating the new processes and procedures with operating SoA/RLVs. The 'safety target' should be based on an Equivalent Level of Safety (ELOS) to that of operating aircraft with the exception of storing and handling propellants. Arguably the exposure to the risks should be identified and from this the Spaceport Authorities should be able to determine the risk of death per person per year (per group of people) as detailed in the ALARP section (3.4.9).

3.5.8 Spaceport Conclusion

Spaceports are indeed emerging all over the world; a few have been assessed by the regulators and can operate as such – the others are Spaceports in name only for the time being. There are Spaceports that are being constructed from new and these have an excellent chance of providing a safe operating base; however it is important for these Spaceports to follow guidelines and also derive Safety Requirements based on other best practice such as from within the aviation aerodrome safety management systems. Additionally these Spaceports should begin with a Safety Management Plan which should kick-off their safety culture and define the safety activities required. It should also be underpinned by a Spaceport safety case in order to ensure all aspects have been covered in providing a safe 'system'. As for current airports that aspire to become Spaceports there are fundamental additional requirements when considering Rocket Propulsion Systems and the integration of spacecraft to the existing Air Traffic Management system.

It is concluded that both of these approaches are achievable as long as the Spaceport operators consider implementing a fully integrated SMS from the beginning and one that engages with the spacecraft operators such that all known hazards and risks can be effectively managed

3.6. REDUCING OPERATOR RISKS – MEDICAL, TRAINING & PROTECTIVE EQUIPMENT STRATEGIES

The review conducted in Sections 2.3.4 and 2.3.6 highlighted gaps in the FAA-AST Rules and Guidelines; this is the current state. To get to a 'future state' the following Medical, Training and Protective Equipment strategies are recommended in order to reduce the risks to flight crew and SFPs (as controls to Inherent Hazards and Inherent Accidents). For each current (FAA-AST) medical or training mitigation there is a 'recommendation' for a more robust strategy and this is then further backed up (where appropriate) by the findings of the Aerospace Medical Association Working Group (AsMA) [69] as discussed in Chapter 2.3.4.

3.6.1 Current Flight Crew Medical Mitigation

The FAA-AST has only stipulated that a Class II medical certificate is required as detailed in the Gap Analysis in section 2.3.4 .

3.6.1.1 Recommended Flight Crew Medical Criterion Strategy

Class I Aerospace Medical Certificate

The Flight Crew medical criterion should be based on the most stringent criterion (during the early phases in particular) and this is a Class I medical certificate. This standard is also what military fast jet pilots must attain due to the exacting environmental stresses imposed on the pilot.

AsMA: A FAA first-class medical certificate using the same age-based schedule as is required for ATP pilots. An FAA first-class medical certification (instead of the current FAA requirement for an FAA second-class certification) differs from a second-class only in that it requires an EKG and has to be renewed every 6 instead of 12 months over the age of 40.

Dosimeter for Radiation Exposure

Flight Crew should be provided with passive radiation dosimeters so that their exposure can be monitored; the author's previous Thesis [65] proposed an annual limit of 50mSv and a career limit of 100mSv (it is anticipated that a typical annual dosage may be in the order of 7-15 mSv). Additionally, Operators should introduce limitations for pilots in terms of maximum dosage over their career.

AsMA: Passive ionizing radiation dosimeters worn by each flight crewmember

Fatigue Management

Flight Crew may fly daily or even twice daily depending on vehicle availability and demand. This may be more exacting on the body than is realized and pilots may suffer fatigue which can lead to human error and subsequent incidents or accidents. Operators should undertake the FRR Risk Assessment as per Table 22 whereby fatigue is detailed and in order to reduce the risk of a flight it may be necessary to provide a pilot who has not flown that day or the day before. Clearly more analysis is required to understand the fatigue involved in suborbital flights.

AsMA: The pilot experience on suborbital flights will be very time intense and probably repetitive with some pilots flying daily. The effects of repetitive exposures to the physiological stresses of suborbital flight have never been experienced.

3.6.2 Current SFP Medical Mitigation

The FAA-AST has only stipulated that a basic medical questionnaire and General Practitioner's medical certificate is required; thus leaving the decision as to the fitness of the SFP down to the Operator's physician (herein after known as the Flight Surgeon).

3.6.2.1 Recommended SFP Medical Criterion Strategy

The decision as to whether a prospective SFP is medically 'fit' should not be left to what the prospective SFP's medical history states (as supplied by the individual's doctor).

SFP Medical

Two-tiered approach of GP Medical BUT with specified questionnaire. This would be followed by the Operator's Aerospace Physician undertaking a medical on arrival. The Operator medical is designed for two reasons; firstly to ascertain whether the SFP can undergo centrifuge experiential training and secondly to be able to participate in the suborbital flight. Figure 62 below details a combined strategy for medical and centrifuge training.

SFP Go/No-Go List

A list containing those medical issues that may contraindicate an SFP from participating in a suborbital flight should be derived and provided in the SoA Policy as guidance material.

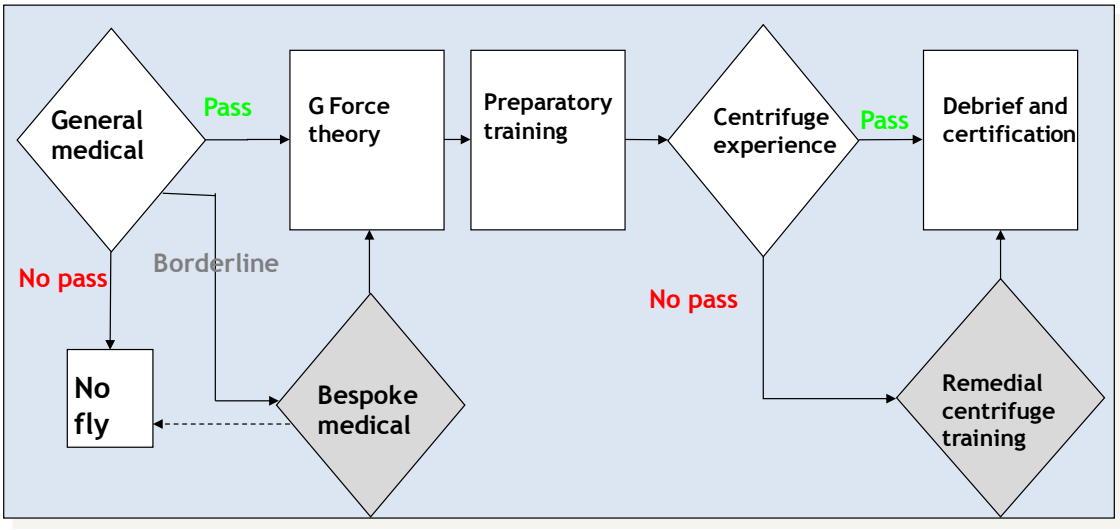


Figure 62: Exemplar Medical and Training Criterion Strategy

Medical Telemetry

Medical Telemetry for both passengers and flight crew on board SoAs could be deemed as an essential requirement; in particular in the early days of flight test and initial flights. It may then become standard practice.

A Flight Surgeon (Aviation Medicine Specialist) should be employed by the Operator to monitor the SFPs and the Flight Crew. Figure 63 below is an example of such a Telemetry system.

Figure 63: Telemetry 'vest' to monitor SFPs and Flight Crew

Recommendation: It is recommended that the IAASS SSS TC undertake analysis based on the findings in 3.6.2 in relation to Flight Crew & Space Flight Participant Medical & Protective Equipment Standards. These recommendations are collated at 6.4.8.

3.6.3 Current Flight Crew Training Mitigation

The FAA-AST Flight Crew requirements for training state that the RLV flight crew should be trained to operate the vehicle so that it will not harm the public and that the pilots should hold ratings to operate one or more aircraft with similar characteristics for as many phases of the mission as practicable. These aspects were reviewed in 2.3.6 along with the requirements to provide a simulator. As mitigation this is considered fairly generic and the FAA-AST tend not to be too prescriptive. However it is considered that in the early phases of development, the regulators should stipulate rigorous standards and these could perhaps over time be relaxed (rather than the other way round due to accidents).

3.6.4 Recommended Flight Crew Training Strategy

The proposed Flight Crew training strategy is to have more explicit requirements in addition to those stipulated by the FAA-AST. As a minimum the following training components are recommended:

Centrifuge Training

The centrifuge is not detailed within the FAA-AST guidelines however it is considered an essential component as part of a training strategy. The benefits of a centrifuge is that it can simulate both Gz profiles (eyeballs down) for the transition between horizontal and vertical flight and Gx profiles (chest to back) for the descent phase. Additionally it is assumed that the SoA pilots will be either test pilots and/or ex-military fast jet pilots who have undergone centrifuge training. However some operators may recruit per the minimum FAA-AST requirements. In either case it will be essential that pilots have centrifuge currency as part of the safety mitigation.

AsMA: Recent centrifuge or other G-training may be beneficial if there is significant (> +3) Gz acceleration forces in the flight and the flight crewmembers do not have adequate +Gz training in other environments.

AsMA: Anti-G suit use on early flights until more experience has been obtained as there will be significant (>3) +Gz acceleration forces in the flight profile and deterioration of +Gz tolerance may

occur due to the "push-pull effect" after several minutes of 0g. There is no data concerning +Gz tolerance following four minutes of 0g.

AsMA: Higher g forces or longer exposures to acceleration could potentially increase the frequency of dysrhythmias. As long as the head, neck and spine are stabilized before the acceleration exposure and remain so until the exposure is completed, the potential for musculoskeletal injury is markedly reduced.

Recommendation: It is recommended that the IAASS SSS TC undertake analysis based on the findings in 2.3.6 and above centrifuge and anti-g suit proposals. These recommendations are collated at 6.4.8.

Simulator Training

The FAA-AST requirements concerning simulator aspects are generally sound and state that the *flight crew training device (*should*) realistically represents the vehicle's configuration and mission.* It is imperative that the simulator accurately represents the vehicle in terms of 'concurrency'; this is whereby the configuration is the same as the aircraft (instrumentation, switches, seats, doors, etc.). The rationale is that the other two attributes of a SoA simulator (fidelity and capability) will not accurately reflect the vehicle and therefore can affect the aim of the training. In terms of fidelity (concerning the visual and motion system and accuracy of the instrumentation) it will be extremely difficult to represent high g-forces in all axes. The simulator will not be able to accurately represent the vehicle's capabilities in terms of the 'pull-up', ascent, space segment (with upside down and reaction control aspects) and the high-g descent. Nonetheless, the simulator is an essential component of flight crew training.

Recommendation: It is recommended that the IAASS SSS TC undertake analysis based on the findings in 2.3.6 and above simulator proposals. These recommendations are collated at 6.4.8.

Parabolic Flight Training

In terms of flight crew training it is considered desirable that they experience microgravity conditions however it is not considered an essential requirement because the flight crew will be strapped in their seats and controlling the flight.

AsMA: Parabolic flight training may be beneficial as it does provide some experience to the acceleration-weightlessness-deceleration environment, although no studies have shown that it contributes to establishing a "dual adaptive" state. Some personnel have experienced motion sickness with the initial exposure to parabolic flight, but develop tolerance with adaptation to the changing gravitational fields.

Altitude Chamber Training

Military fast jet pilots (and all other aircrew) are trained to recognize the signs and symptoms of decompression so that they can carry out emergency procedures, including donning an oxygen mask and switching to 100% oxygen under pressure breathing conditions. This is also considered essential for Suborbital flights because the flight crew must be able to respond to the earliest indications of pressurisation problems in order to maintain control of the vehicle. The altitude chamber provides simulated pressurisation failures by climbing the 'chamber' to 25,000 feet (ft.), 45,000ft (pressure breathing is required at this altitude) and the author has observed an altitude of 100,000ft in a chamber (though this was for experimental purposes and no-one was inside the chamber).

AsMA: Physiologic training (altitude chamber) to ensure flight crew recognition of signs and symptoms associated with decompression including hypoxic changes.

Recommendation: It is recommended that the IAASS SSS TC undertake analysis based on the findings in 2.3.6 and above altitude training proposals. These recommendations are collated at 6.4.8.

3.6.5 Current SFP Training Mitigation

The FAA-AST has only stipulated that a basic training is required for SFPs in the form of briefings; thus the individual's would not know ether they could cope with the nominal (and non-nominal) 'g' forces during the flight. The FAA-AST guidelines for Flight Crew training are slight better but still require further refinement and to be more explicit in some instances.

3.6.6 Recommended SFP Training Strategy

As per the flight crew training strategy, the SFP training strategy must have more explicit requirements than those stipulated by the FAA-AST. The SFP training strategy should include the following:

Briefings:

Space Awareness briefing; this should consist of various videos on the history of human spaceflight, including space tourism, and also provide a tutorial on the space environment and explaining the rationale for some of the training that SFPs will encounter (detailed below)

SoA briefing; this briefing should be explicitly related to the SoA that the SFPs will fly in. It should include the basic attributes of the vehicles both on the ground and in the air. This should include a video and possibly mock-ups in the classroom environment in order to familiarise the SFPs with the vehicle.

Emergency briefing; this briefing, once again in the classroom environment, should concern the vehicles safety equipment (fire extinguishers, goggles, oxygen masks, protective clothing) and the actions that SFPs should take in an emergency. SFPs should then be given a 'safety information' booklet that they can study.

Centrifuge Training

As per flight crew, the centrifuge is not detailed within the FAA-AST guidelines however it is considered an essential component as part of a training strategy. The benefits of a centrifuge is that it can simulate both Gz profiles (eyeballs down) for the transition between horizontal and vertical flight and Gx profiles (chest to back) for the descent phase. In terms of SFPs this is essential because, unlike the pilots/flight crew, they will not have experienced sustained g-forces. They will also not have received training in carrying out an 'Anti-G Straining Manoeuvre (AGSM).

Simulator Training

The simulator is an excellent training tool for the flight crew but in the case of Suborbital flights it can also be an essential part of the SFP training strategy. Having received briefings about the vehicle, the SFPs can then be physically trained on the equipment in terms of the following;

- Normal Ingress/Egress; it is important that the SFPs are familiar with the basic configuration of the vehicle and are able to enter and exit
- Operation of Seats; the seats (and restraint system) may actually save their lives so a demonstration and practice in the use of the seat and restrain system is vital.

This may be even more important if the seats are designed to recline with certain phases of flight to assist in countering the effects of g-forces.

- Operation/Procedure for returning to seat (after microgravity phase); should SFPs be allowed to 'float' in the short duration of microgravity then it will be essential that they return to their seat and are restrained for the descent phase. If this does not occur it is envisaged that they will naturally be forced to the floor under the g-forces; this may have dire consequences should another SFP also be forced on top of another SFP as this would result in experiencing twice the weight of the person on the chest resulting in injury or indeed death.
- Emergency Training
  - Pressurisation failure; depending on the vehicle and operating requirements in the event of a pressurisation failure during the rocket phase and microgravity phase then the vehicle occupants will be in grave danger. This failure condition should then provide a logical argument to provide the occupants with a pressure suit and person oxygen system. The SFPs will then be trained to either shut their helmet or select 100% oxygen (or indeed this may happen automatically). In this instance it is important that SFPs receive full training in the use of their 'spacesuit' and in particular what to do in the event of a pressurisation failure. The author has first-hand experience from the altitude chamber in pressure breathing and it is extremely difficult for 'first-timers' (pilots are used to this).
  - Fire; in the event of a fire whilst airborne there is little the flight crew will be able to do as they will be trying to land the vehicle as quickly and safely as they can. This therefore leads to the issue of fire-fighting. In the event that there is no 'cabin crew' (this would be a good argument to having cabin crew) then it would be up to an SFP to attempt to fight the fire. This leads on to training in the use of the fire-fighting equipment, which could be an issue with some SFPs not being physically or mentally able to do this.
  - Loss of control; as occurred on the X-Prize flights, Space-Ship One had an instance of roll 'runaway'. This non-nominal situation could occur on flights and although pilots are trained and used to this sort of manoeuvre, SFPs are certainly not. During the rocket phase and descent phase SFPs should be restrained in their seats and this should not normally be an issue; though it is worth briefing SFPs on and demonstrating the use of a possible 'locked' position of the restraint system.
  - Crash Landing; this event could occur from a loss of control incident or other flight events and as per normal aviation a procedure should be implemented and then practiced in the simulator for the SFPs to 'adopt the position' (if appropriate).
  - Emergency Egress; in the event of the crashed landing then the SFPs may have to egress quickly. This may involve unstrapping normally or there may be a Quick-Release Button, followed by exiting the vehicle. Once again this can be practiced in the simulator.

In terms of emergency training some operators may feel that demonstrating too many of these aspects may frighten SFPs and so may wish to selectively omit some training. It is considered that the characteristic type of the SFP is an 'adventure seeker' and in fact that they will demand to be involved as much as possible and to undertake as much training as is required. Operators should not reduce safety training as part of cost cutting.

Parabolic Flight Training

Although not essential for flight crew, should SFPs be allowed to leave their seats in the microgravity phase of the flight then it is considered essential that they have parabolic flight training. The XCOR

Lynx[29] vehicle for instance is a two-seater cockpit (one pilot, one fee-paying SFP) and in this instance as the SFP will not be leaving the seat then there is no requirement for parabolic flight training.

Psychological Training

The physiological training elements detailed above will undoubtedly provide psychological benefits for the SFPs in overcoming any fears or concerns regarding the flight. Indeed much can be done to prepare the SFP for their once-in-a-lifetime experience including a countermeasures program. Professor Robert Bor [100] has such a program for aviation and this sort of approach could be adopted by operators:

- *Education about the physical principles of flight and the process by which the flight crew control the aircraft*
- *Experiential learning through participating in a simulated or actual flight situation*
- *Training and techniques to manage the physiological symptoms of anxiety*

Another psychological benefit of the physiological training is that the SFPs will feel properly integrated with the flight crew and it will no doubt feel for of a team mission rather than a mere individual 'joy-ride'.

Recommendation: It is recommended that the IAASS SSS TC undertake analysis based on the findings in 2.3.6 and the above SFP proposals. These recommendations are collated at 6.4.8.

3.6.7 Risk Reducing Equipment

The review in Chapter 2.3.4 highlighted a number of 'inherent' issues that flight crew and SFPs will be subject to and some of these have been discussed above as medical and training issues. The final risk reduction methods concern ancillary protective equipment in order to prevent inherent hazards and accidents:

Noise Reduction

The reviews and discussions above highlight the noise issue during the 'launch' or rocket phase and even though this may only be for 90 seconds it can have an impact on safety and on comfort. To reduce the risk from this hazard the mitigation should include: Fully enclosed Space Helmet + effective circum-aural seals + Active Noise Reduction (ANR) + Communications Ear-Plugs (CEP):

- Fully enclosed Space Helmet with/or,
- Effective circum-aural seals and,
- Active Noise Reduction (ANR) or
- Communications ear plugs (CEP)

AsMA: Auditory protection in the helmet or headset for all crew members

Anti-Vibration Measures

the rocket phase will not only result in excessive noise it will also result in a marked level of vibration. The hazards associated with vibration will not only affect the individual but will also affect the performance of the flight crew. Mitigation measures should include:

[29] http://www.xcor.com/

- Anti-vibration mounts on the cockpit console
- Anti-Vibration seats
- Seats with shaped head rests to prevent the flight crew's helmet moving in the lateral sense

AsMA: Mitigation strategies for reducing vibration would be to aggressively decrease vibration in the design of the vehicle, isolate the pilot by seat design, and the use of a helmet to isolate the head which has been shown to improve display reading performance and vibrational tolerance[30]

Pressure Suits

Should the cabin suffer decompression during the rocket phase or the 'space phase' then the occupants are likely to suffer death leading to a loss of the vehicle as well. Passenger aircraft do not need this as they can deploy and emergency oxygen system and reduce the aircraft's height rapidly to below 12,000 ft. Although designers (like Scaled Composites) believe that a 'shirt-sleeve' environment is preferred (to demonstrate that their design is robust) there is always the likelihood of a catastrophic failure of the pressurised vehicle and therefore appropriate mitigation should be adopted:

- Flight Crew should have full pressure suits (especially during early phase of flights)
- SFPs should have partial-pressure suits or specially designed suborbital spacesuit for emergency situations (see 4.1.2)

AsMA: Pressure suit use may be adopted by some commercial space flight operators as it would be beneficial in the case of failure of the pressurized vehicle. Without a pressure suit the crew is absolutely reliant on cabin integrity being maintained as there is no redundancy and depressurization would be a catastrophic event.

Anti-G Suits

From personal experience, the purpose of anti-g trousers is twofold: it gives an extra 1-2G protection and it also gives the wearer notice of the onset of 'G'. This would benefit the pilot and help reduce the workload. In terms of SFPs there may be a case for anti-g trousers depending on aircraft design and flight profile. Alternatively the SFPs could have tight-fitting 'long-johns' (undergarments) and zipped gaiters as part of their spacesuit (or as part of special spaceflight coveralls if no spacesuit).

AsMa: There are currently no plans to utilize anti-G suits similar to the Shuttle pilots during re-entry on these flights, but could be considered for the pilots as the cost is minimal and a beneficial effect is possible.

Dosimeters

The authors Thesis [65] found that although the radiation exposure levels have been shown to be negligible for participants and small for pilots, there is still a risk for the pilot over a period of time. There should be a career limit for exposure to ionising radiation (100mSv career limit for the pilots per the Authors' findings) and this can be achieved through wearing a dosimeter and recording each flight crew member's exposure. Further mitigation can then be crew scheduling as an individual starts to reach the limit.

[30] AsMA paper referencing; Taub HA. Dial Reading Performance as a Function of Frequency of Vibration and Head Restraint System. AMRL-TR-66-57> Wright Patterson AFB. Aerospace Medical Research Laboratory. 1966.

AsMa: All flight crewmembers should be required to wear personal dosimeters to track an individual's accumulated dose for each mission, as do radiation workers and medical imaging personnel, to ensure compliance with OSHA standards

Fire Fighting Equipment

Should the hazard analysis identify that there is a possibility of an on-board fire then risk reduction methods need to be employed. One such method is by providing fire-fighting equipment (extinguishers) and where appropriate fire detection and warning systems (such as in avionics bays). Access should be provided if possible to potential fire-risk areas and the flight crew should be provided with personal protective equipment such as fire-gloves.

Medical Emergency Equipment

Although a suborbital flight is considered a short-duration event there may be circumstances where medical equipment is identified as a risk reduction measure. The main factor in the identification of this aspect is vehicle design; clearly XCOR's RLV with one passenger and one pilot strapped in with a profile that transports the occupants to suborbital apogee in 15 minutes may not require medical equipment. However a design and flight profile such as Virgin Galactic's will afford sufficient time to enable first aid to be conducted. Additionally this may be even more appropriate should the spaceport be in a remote location such as Spaceport America in New Mexico; here the medical facilities may be able to cope with small emergencies but the nearest hospital is 2-hours away.

3.6.8 Summary of Proposed Operating Mitigation Measures

The reviews conducted in Chapter 2.3.4 and 2.3.6 and the proposed guidelines in Chapter 3.6 above are important in terms of medical, training and personal equipment mitigating strategies (or operator safety controls), but these must be focused and managed within the accident sequence. The following table assimilates the issues and mitigation measures discussed within this Chapter to specific hazards or accidents as appropriate.

Note: A hazard control attempts to prevent the hazard occurring and therefore an accident control attempts to prevent the accident occurring i.e. the hazard already exists.

Section	Issue/Cause	**Hazard Control**[1]	Associated Hazard	**Accident Control**[2]	Associated Accident[3]	Accident Severity
3.6.7	Noise from rocket	Internal soundproofing	Exposure to excessive Noise	Helmet	Musculoskeletal (temporary loss of hearing)	Negligible
3.6.7	Noise from rocket	Helmet with ANR and CEP	Loss of/ Degraded Communication		Loss of Situational Awareness	Catastrophic
3.6.7	Vibration from rocket	Anti-vibration seats	Exposure to excessive Vibration		Musculoskeletal (pains) Cardiopulmonary (restricted breathing)	Major
3.6.7	Vibration from rocket	Anti-vibration seats Anti-vibration mounts for cockpit console	Impaired ability to read instruments		Loss of Control	Catastrophic
3.6.7	Hull/window crack		Decompression	Pressure Suits Altitude Chamber training (pilots)	Asphyxiation	Catastrophic
3.6.7	Hull/window crack	Design - Double skin Design - load factors	Primary structure failure		Structural failure	Catastrophic
3.6.7	Flight in ionising radiation	Design - Double skin	Exposure to ionising radiation	Procedure -Dosimeter for pilots Limitation – Career limit for pilots Limitation – flight in known solar flare prohibited	Musculoskeletal	Hazardous-Major
3.6.7	g-forces	Design – Seat to recline position	Exposure to excessive g-forces	Anti-g suit Centrifuge Training	Cardiovascular (G-LOC leading to death)	Hazardous
3.6.7	g-forces		Exposure to excessive g-forces	Anti-g suit Centrifuge Training 2-pilot operations	Loss of Control	Catastrophic
3.6.7	O_2 and CO_2 build up	Ventilation (blower)	Exposure to Hazardous/Toxic Materials	Pressure suit/helmet/with oxygen system (plus 100% emergency oxygen)	Asphyxiation	Catastrophic-Hazardous
3.6.7	Many causes	Design certification/ qualification of equipment	Cockpit/cabin Fire	On-board fire fighting equipment Warning System	Fire/Explosion	Catastrophic
3.6.7	Vehicle design	Design	Slips & Trips	Simulator training (includes briefing and demonstration)	Musculoskeletal	Major-Minor
3.6.7	Inherent Flight profile		Space Motion Sickness	Parabolic flight training Centrifuge training (Gx)	Neurovestibular (sickness)	
3.6.7	Inherent Flight profile	SFPs to take SMS tablets (not pilots)	Space Motion Sickness	Perspex (clear) barrier between SFPs and flight crew (prevents vomit from ‘floating’ to cockpit which could impair pilots ability to fly	Loss of Control	Catastrophic

Table 23: Operator Risk Reduction Measures – against specific hazards or accidents

Notes: (1) Hazard control is an attempt to prevent the hazard occurring. (2) Accident control is an attempt to prevent the accident occurring. (3) The Accidents are from the proposed Accident Lists (Table 12)

CHAPTER FOUR – Synthesis of Emerging Technologies

4. INTRODUCTION

This Chapter aims to provide discussions on emerging technologies within the Suborbital domain. The topics chosen are based on issues that have been discussed at conferences and from the author's viewpoint. Additionally the opportunity arose to analyse a different approach to personal spaceflight – that of the challenges in providing a safe mode of transport almost to space ('near space') in a helium-powered balloon.

4.1. SPACESUITS

Historically spacesuits were designed for operations on the Space Shuttle or on the Soyuz spacecraft. With the emergence of the suborbital flights a new approach is being considered – to fly with or without spacesuits.

4.1.1 NASA Designs

Spacesuits are essential for astronaut protection during launch, re-entry and of course during extra-vehicular activities (EVA). Additionally during visits to the International Space Station (ISS) astronauts require spacesuits in case of emergencies on board. In discussions with the astronaut Mario Runco[31] he stated that one of the main issues was the fact that the spacesuit was a two-part suit and also that the gloves hampered operations. It is not envisaged that NASA-style pressure suits would be suitable for the smaller suborbital craft.

4.1.2 Suborbital Specific

In terms of suborbital flights there are discussions 'for & against' spacesuits and these may be operator and vehicle specific. Indeed Virgin Galactic passengers may wish to have spacesuits (to look the part) whereas Burt Rutan (the designer from Scaled Composites) was cited as wanting passengers to fly in a 'shirt-sleeve' environment; this was probably his way of stating that his design is safe. Nonetheless it is an issue that requires further discussion. The argument against having pressure suits would be that the hull (including windows) was double-skinned and therefore the design is robust – this is the argument Virgin Galactic and Scaled Composites are debating.[32] It is considered by the author that the early flights should have pressure suits until the SoA/RLVs have proven reliability. The issue was also discussed in 3.6.7 with a recommendation for further analysis as part of the IAASS SSS Technical Committee. Figure 64 below shows a spacesuit designed by Orbital Outfitters [101] for the suborbital market and this comes with various safety features in order to '*provide a line of protection in the event of a loss of atmospheric pressure within the vehicle'*:

- *Has an automatic rapid activation function*
- *The design provides an independent 15 minute back-up*
- *Has in-built communication system*
- *Has an integrated sensor system to record real-time biometric information*
- *Can be integrated into a parachute harness*

[31] Mario Runco was a guest speaker at the first 'Manned Space Flight Course' in Sweden, Aug 2006
[32] As stated by Jim Vanderploeg (Virgin Galactic Chief Medical Officer) at the 2nd IAA Conference, Arcachon, 30 May – 1 June 2011

Figure 64: Suborbital Spacesuit by Orbital Outfitters

The benefit of this spacesuit (for the suborbital domain) is that credit can be taken for the great safety features because they are real life-saving mitigation factors.

SoA/RLV operators (and designers) should undertake analysis per the *SATURN SAFETY MODEL* which is a contiguous approach from designer to operator, and they would then be able to complete the accident sequences properly. By this it is meant that the operator could complete an Event Tree Analysis to demonstrate that in the event of a loss of pressurisation that there are further mitigation to prevent the death of those on board (and in particular the flight crew who could then prevent the loss of the vehicle and therefore the outcome would be a Serious Significant Event (SSE) as opposed to a real accident (Loss of Control due to pressurisation failure resulting in loss of all on board and loss of vehicle).

Optimisation Analysis

Optimisation analysis is whereby the potential controls are listed and then analysis is undertaken to determine which of the controls are taken forward. There are two safety-based techniques that can be applied; cost benefit analysis (CBA) or decision analysis and these should be backed up by a sensitivity analysis.

Cost Benefit Analysis (CBA)

CBA[33] is used in the UK's Health and Safety Executive's ALARP process [56] whereby the benefits gained are all defined in terms of monetary costs; this is known as the ALARP Budget i.e. it is how much a duty holder should spend in order to reduce a residual risk to ALARP. The HSE define CBA as:

> *"It is a defined methodology for valuing costs and benefits that enables broad comparisons to be made between health and safety risk reduction measures*

[33] http://www.hse.gov.uk/risk/theory/alarpcba.htm

on a consistent basis, giving a measure of transparency to the decision making process"

There are various ways of calculating the cost and the metrics involved for aircraft/SoA related systems will include the following. As an example some assumed and arbitrary figures are provided for a SoA and these are shown in brackets:

- P = Probability of the accident (associated with a failure condition) [$1x10^{-5}$ per flying hour]
- E = Exposure to the Risk through life [2500 – SoA designed for 5 year life with 500 predicted hours per year based on 5 vehicles flying 100 hours each per year]
- V_H = Value of 1 occurrence in human terms i.e. Number of people involved times value of prevented fatality or injury (whether flight crew, spaceflight participants or public) [2 flight crew plus 6 SFP = 8] times £3M arbitrary value of life as an example = £24M
- D_F = Disproportionality Factor [6 – this is based on a C Class medium Risk]
- V_A = Value of 1 occurrence in non-human terms (for loss of asset – this is not included for inherent people accidents) [£20M]

The ALARP Budget is worked out thus:

$(P \times E \times V_H \times D_F) + (P \times E \times V_A)$ [Equation 5]

= £3.6M + £500,000 = £4.1M

This means that for this particular accident (as a result of a failure condition or inherent hazard – in regards to flight crew or SFPs dying as a result of loss of pressurisation) the operator (duty holder) should be prepared to spend £4.1M to reduce the risk of death to the flight crew and/or SFPs. The value of the asset (V_A) is not included if the analysis concerned the SFPs only; whereas if the flight crew were incapacitated then the vehicle may be lost and so the value is added. This can also be argued as the reason to provide flight crew with spacesuits; the argument for SFPs could be claimed by CBA or by 'decision analysis' (see below).

The next stage is to determine the actual cost of the spacesuits in this instance and this should be the total through-life cost. Let us argue that the Orbital Outfitter's spacesuit is £500k each including through-life costs. With eight people on board this comes to £4M and therefore is under the ALARP Budget; ergo the duty holder should introduce spacesuits as the control measure. If the spacesuits were £5M each then at £40M total cost this could be argued as '*grossly disproportionate'* i.e. the cost far outweighs the benefits gained. Either way in this case the factor may be simply down to a society-based decision.

Note: the values and equation used here represents a simplified method in order to demonstrate the principle of CBA in the ALARP process. There are far more comprehensive methods using spread-sheets to include all of the variables involved such as training, lesser severity accidents and so on.

Decision Analysis

In the case of the spacesuit it might be more socially or politically acceptable that SFPs (and in particular flight crew) are provided with spacesuits and this is simply a decision made by the duty holder. This is probably the case with Virgin Galactic in that Burt Rutan wanted a 'short-sleeve' environment whereas the Virgin Galactic team (and their customers) wanted to look like an astronaut.

Sensitivity Analysis

Once the CBA has been conducted a sensitivity analysis should be undertaken in order to assist the duty holder with the decision where uncertainties prevent a final decision. The HSE define this activity as:

> *"A sensitivity analysis consists of varying one or more of the parameters/assumptions of the CBA to see how these variations affect the CBA outcomes"*

In the example above should the probability be reduced to $1x10^{-6}$ per flying hour as part of the sensitivity analysis then the ALARP Budget is reduced to £320,000. Or if the number of people on board was limited to 6 and the Value of life reduced to £2M then the ALARP Budget is £3.2M.

4.2. EMERGENCY SYSTEMS

Emergency systems are required on normal aircraft and in terms of the aircraft crash landing or ditching, these range from airworthiness seats to escape slides and dinghies. Designers and Operators should be discussing emergency systems from the outset in a development program and requirements should stem from User Requirements and fed down to System Requirements. From a bystanders point of view it would appear that designers like Scaled Composites have adopted a 'solution-based' approach rather than having a customer in the first instance determining what the User Requirements are. Indeed what are Designers doing to decide whether or not they should incorporate emergency systems such as a Ballistic Recovery System – it could be argued that to demonstrate that they have reduced their Risks to as low as reasonably practicable (ALARP) they should provide quantitative analysis i.e. using the CBA technique as described above.

In a presentation on Crew Survivability, Jonathon Clark[34] gave a moving account of how it was possible that the Crew of the Space Shuttle Columbia would have been alive (but possibly unconscious) after the craft broke up and was hurtling to the Earth. He stated that rather than 'emergency' and 'rescue' capabilities that Spacecraft should feature survivability measures as this was the most likely of the choices of mitigation for post-accident mitigation.

Ballistic Recovery System

A Ballistic Recovery System (BRS) is essentially a parachute system that deploys in the event of a loss of control emergency and the aircraft/spacecraft then parachutes safely to the ground. Figure 65 details a BRS deployed on a General Aviation aircraft. To date the BRS has saved 261 lives[35].

[34] Presentation at the 2nd IAASS Conference, Chicago, July 2007, "*Crew Survivability: The New Frontier of Safety by Design in the Post Shuttle World*," Jonathon Clark's wife was an astronaut on board of Space Shuttle Columbia.
[35] 261 lives saved as at 25 Apr 2011: http://www.brsparachutes.com/lives_saved.aspx

Figure 65: Ballistic Recovery System

Arguably if a Suborbital Aircraft/Reusable Launch Vehicle is in an uncontrolled ballistic descent then the BRS would have to be capable of arresting the fall and maintaining structural integrity of the BRS-to-aircraft connectors. In addition to BRS as mitigation for the SoA/RLV it could be used for personal jettison pods as describe below.

Personal Parachutes

Personal parachutes are used with gliders and arguably most current SoA/RLV designs have a 'glide approach and land' model and so parachutes could be introduced as part of safety mitigation (see 4.4.8 under Hot Air Balloons). Additionally high-performance aircraft 'thrill rides' can be undertaken by the general public and they are provided with a parachute in case of emergency.[36] Sports Parachutists and military parachutists have a main parachute and a reserve parachute. There are various methods of opening the parachutes ranging from static-line release to automatic altitude release systems. The reserve parachute is operated in the event of main parachute failures. In terms of parachutes for people flying in gliders they only have one parachute as this acts as the 'reserve' in case of aircraft failures.

It is interesting that the spacesuit designer (Orbital Outfitters) state that their spacesuit '*can be integrated into parachute harnesses'*; this ratifies the author's view that parachutes should be used as a personal safety feature for suborbital flights (meaning that other safety-minded engineers think in terms of mitigation – the spacesuit is a control and so is a parachute).

Jettison Sphere/Seats

In military fast jets pilots are provided with an ejection seat because of the high speed at point of ejection i.e. they are 'assisted' in leaving the aircraft by means of a rocket-fired ejection seat. To further assist the pilot in safely ejecting the canopy is also ejected or it is removed by detonation via miniature detonation chord.

[36] http://www.extrabatics.com/Thrillrides.aspx

To implement such a system in a suborbital aircraft would depend on the design of the vehicle. In standard business-jet SoA such as the EADS-Astrium vehicle carrying six passengers this would not be practicable. However the XCOR Lynx I & Lynx II RLV is a two-seater vehicle with the passenger sitting alongside the pilot. In this instance the vehicle could be designed to have ejection seats and this would be particularly relevant to the Lynx vehicles because the vehicle is rocket-powered from the runway. In the event of an abort scenario of Loss of Control or Fire then the occupants would be able to escape.

In terms of a Jettison Sphere, these would be more relevant to orbital systems or could be employed on suborbital aircraft should the design have this in mind from the beginning. In particular jettison spheres could be a practical solution for vertical take-off and landing vehicles such as Blue Origin's 'Sheppard' RLV. Here, if the SFPs are positioned around the circumference of the hull then they could be secured in a personal 'pod' for take-off and landing and this could also be a jettison-able pod. The pod would then have a BRS as the means to arrest the fall and bring the SFP safely to the ground.

4.3. ROCKET PROPULSION SYSTEMS

4.3.1 Rocket Propulsion

The various suborbital spacecraft designs have different Rocket Propulsion Systems (RPS) with some based on existing technology and some having new and innovative designs. The RPS is the heart of the spacecraft and this is the most technically challenging aspect in designing new suborbital spacecraft. There are different RPS models being developed for the suborbital market and the following presents a summary of the basic types of rocket motors and their propellants:

Liquid Rockets

Liquid Rocket Propellant is a common type of propellant which yields the highest specific impulse (I_{sp}) i.e. the efficiency of the rocket motor (analogous to miles per gallon) in terms of impulse per unit of propellant. In Liquid systems both the fuel and the oxidizer (also a liquid) are brought together in the combustion chamber and ignited. Liquid propellant was used on the Space Shuttle and in the stages of vertical rockets such as Ariane 5 and Delta IV[37] and due to the reliability factors liquid propellant is being used as a natural progression within some suborbital rocket motors. Some common liquid-fuel combinations include:

- Liquid Oxygen (LOX) and kerosene (commonly known as RP-1);
  - XCOR's Lynx RLV uses this type of propellant. Additionally XCOR are making progress with their cryogenic LOX pump and stated at the 2nd IAA that they had bench-tested it for 8 hours with no wear and therefore after testing were estimating a reliability rate of 5000 hours.
  - Rocketplane XP will also use LOX-Kerosene
  - EADS-Astrium's space-plane will also use LOX-Kerosene
- LOX and methane;
  - Armadillo Aerospace use this type of propellant in their MORPHEOUS VTOL vehicle

Liquid Rocket Issues

[37] http://en.wikipedia.org/wiki/Liquid_rocket_propellants

Issues with Liquid rockets (as with jet engines) is that they require ignition immediately it is selected otherwise too much liquid will be in the combustion chamber and then they can either fail to start or should ignition occur late then a fire can occur (wet start) or within a pressure vessel a catastrophic failure may occur due to the excessive pressures (hard starts).

Handling and Storage of LOX can be problematic but well-practised procedures can help mitigate some of the issues.

Hybrid Rockets

Hybrid Rockets use two different sorts of propellants in different states normally comprising of one solid and the other gas or liquid. As opposed to the Liquid system the solid portion of the hybrid system is already in the chamber and the generally the oxidizer is injected into the chamber and ignited. Figure 66 below details a typical hybrid rocket motor configuration[38]. The solid fuel used in Space Ship One was rubber and the liquid oxidizer was 'laughing gas' or Nitrous oxide (N_2O).

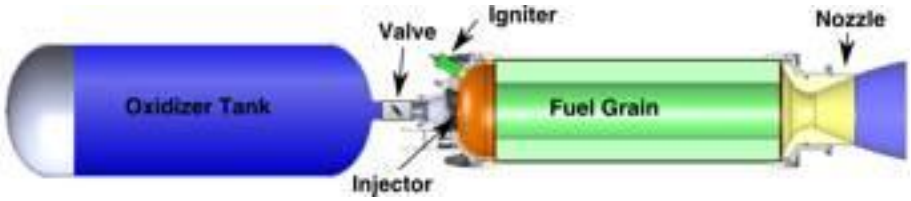


Figure 66: Typical Hybrid Rocket Motor

Hybrids tend to combine the safety features and advantages of both solid fuel and liquid fuel rockets and therefore could be construed to be safer; in particular in the storage of the solid fuel.

In Kenny Kemp's book [15], he discusses the Virgin Galactic hybrid rocket motor with George Whitesides (Virgin Galactic Chief Technical Officer in 2007, now Chief Executive Officer):

> *"The beauty is that because the propellants are separated physically and by phase – meaning one is a liquid and one is a solid – they cannot intimately mix in the event of a leak or something going wrong. So consequently, they cannot explode. They can't detonate and they are very failure-tolerant. If the fuel inside a motor case cracks, it is not catastrophic the way it is with solid rocket propellant. Composite is the favoured way to go because it is very lightweight and very tough. And because the solid fuel lines the case on the inside, it acts as insulation. You have 5,000 degrees temperatures on the inside but there is all the fuel between the intense heat and the outer casing. The fuel slowly burns away, so the side of the case never feels the fierce combustion temperatures. The case does not see extreme temperatures until the very last moment when you are done"*

Today however the design of the Spaceship 2 rocket has evolved and it is considered by fellow enthusiasts that it is the rocket design that is holding up the program due to various issues; this is

[38] http://www.spg-corp.com/space-propulsion-group-resources.html

partly corroborated by the fact that the test phase has only recently begun and has not yet involved the rocket.

Hybrid Rocket Issues

In theory hybrid rockets should be safer and more cost-effective than their liquid rocket counterparts as long as they are carefully constructed. Indeed filling the solid fuel chamber with the oxidizer (say in the case of a valve leak) would not necessarily explode and therefore the explosive equivalence is often quoted as 0%[39].

The issues mentioned above concerning Virgin Galactic (Scaled Composites) and in particular their accident involving cold-flow tests is a reminder that rockets are however volatile and can explode unexpectedly. Issues with hybrid rockets are (from footnote):

- *Pressure vessel failures; Chamber insulation failure may allow hot combustion gases near the chamber walls leading to a "burn-through" in which the vessel ruptures*
- *Blow-back; flame or hot gasses from the combustion chamber can propagate back through the injector, igniting the oxidizer and leading to a tank explosion*
- *Hard Starts; An excess of oxidizer in the combustion chamber prior to ignition, particularly for monopropellants resulting in a temporary over-pressure or "spike" at ignition*

Table 24 below compares the liquid rocket propellant with those of the hybrid[40] (encompassing both liquid and solid fuels) and details some safety additional considerations.

Rocket	Description	Advantages	Disadvantages	Safety Considerations
Liquid	*Propellant (such as hydrazine, hydrogen peroxide or nitrous oxide) flows over a catalyst and exothermically decomposes; hot gases are emitted through nozzle.*	*Simple in concept, throttle-able, low temperatures in combustion chamber*	*catalysts can be easily contaminated, monopropellants can detonate if contaminated or provoked, Isp is perhaps 1/3 of best liquids*	Handling of LOX – procedures and training must be effective
Solid	*Ignitable, self-sustaining solid fuel/oxidiser mixture ("grain") with central hole and nozzle*	*Simple, often no moving parts, reasonably good mass fraction, reasonable I_{sp} A thrust schedule can be designed into the grain.*	*Throttling, burn termination, and re-ignition require special designs. Handling issues from ignitable mixture. Lower performance than liquid rockets. If grain cracks it can block nozzle with disastrous results. Grain cracks burn and widen during burn. Refuelling harder than simply filling tanks.*	storage of the solid fuel safer but handling/refuelling has issues
Hybrid	*Separate oxidiser/fuel; typically the oxidiser is liquid and kept in a tank and the fuel is solid.*	*Quite simple, solid fuel is essentially inert without oxidiser, safer; cracks do not escalate, throttle-able and easy to switch off.*	*Some oxidisers are monopropellants, can explode in own right; mechanical failure of solid propellant can block nozzle (very rare with rubberised propellant), central hole widens over burn and negatively affects mixture ratio*	Issues with 'spikes' at ignition and so pressure vessel must incorporate good safety margins Also low-frequency pulses noted on Space Ship One flight

Table 24: Comparison of Rocket Motor Propellants

[39] http://en.wikipedia.org/wiki/Hybrid_rocket
[40] http://www.spg-corp.com/space-propulsion-group-resources.html

Propellant Accidents

The above sections highlighted strengths and weaknesses of types of rockets and their propellants and this section will summarise the accidents associated with propellants and in particular during the RPS ignition phase whether in flight or on the launch pad.

The accidents involving the RPS tends to be catastrophic and this was the case for Space Shuttle Challenger (1986) and on the launch pad for a Soyuz T-10 (1983) [see Table 2 and Table 3]. The Scaled Composites accident whilst testing their hybrid rocket system killed 3 of their scientists and severely injured more. Scaled Composites then published lessons learned [13] from the accident in the hope that industry will learn from the dangers of Nitrous Oxide. Key points included:

- *Adiabatic Compression; Designs should attempt to minimize adiabatic compression in the system during flow of the N2O oxidizer.*
- *Decomposition in Liquid; the system pressure significantly affects the ignition sensitivity of liquid N2O. For example, N2O flowing at 130 psi in an epoxy composite pipe would not react even with a 2500 J ignition energy input. However, at 600 psi, the required ignition energy was only 6 J.*
- *Pressure Vessel Design; In the event that ignition prevention measures and deflagration wave mitigations fail, pressure vessel designs should allow for a controlled failure upon overpressure. In large oxidizer systems operated at high pressures, the energy released during a tank rupture for whatever reason (structural, overpressure, feedback, decomposition) is very high. This failure mode should be designed for with burst disk or other similar safety precautions that can safely reduce the PV energy in the vessel without catastrophic failure.*

The Accident (according to the exemplar accident list at Table 12) is clearly accident A5 ‘Explosion’.

- An explosion would results in the following effects:
  - Explosive blast resulting in;
    - Debris from an explosions which may injure or kill support personnel nearby (if on the launch pad or runway)
    - Damage to the vehicle
    - Damage to nearby equipment/buildings
  - Heat energy resulting in;
    - Burns (thermal radiation) to personnel inside the vehicle or to support personnel nearby (if on the launch pad or runway)
    - Fires to surrounding property
  - Release of toxic gases resulting in;
    - Pulmonary Function disorders (difficulty in breathing) leading to asphyxiation
    - Exposure to hazardous/toxic materials (absorption through skin)

Accidents can also happen whilst in the Storage and Transportation phases and this was covered in the Spaceport section at 3.5.

Conclusions on RPS

Rocket Propulsion Systems are arguably the most hazardous and least reliable systems that will be part of a suborbital vehicle and therefore this requires the most effort from the early design phase and throughout the lifecycle; User and System Requirements must be detailed and Safety Requirements must be stated and linked to these primary requirements; then after the initial functional hazard

analysis further derived safety requirements will flow down to the RPS and further still to sub-systems of the RPS. The design and manufacture must follow best practice and the use of materials must be considered carefully. The test phases must be treated with the utmost diligence and even simple cold-flow tests must follow stringent operating procedures encompassing all necessary mitigation such as segregation (of man and machine i.e. distance and shielding), personnel protective equipment, warnings and cautions. Handling propellants must also follow the same rigorous process in particular for LOX and cryogenic equipment.

Even with well-defined engineering and operating procedures the above section highlights that systems safety management can play a role in assuring safety with safety-specific techniques; in this instance Operating and Support Hazard Analysis (OSHA) and Occupational Health Hazard Analysis (OHHA). The OSHA in particular would examine the procedures from a safety perspective, looking for human factor errors (where people skip steps or the procedure is actually in the wrong order or missing a step) and also looks at the concurrency and complexity of tasks and takes into account the environmental conditions for the RPS tests or activities.

4.4. NEAR SPACE BALLOONS

Space Balloons may seem a strange conception but they have been in existence for decades. The early 'high altitude' balloons were used for weather data gathering and later were developed to carry humans prior to the Russian success in sending a human into space using rocket-power. Since then there have a only been a few high altitude balloon flights with humans on board; in particular the 'Excelsior III' balloon used for his third and record-breaking high-altitude 'jump' by Colonel Joseph Kittinger on 16 Aug 1960 from a height of 31.3km[41].

The FAA defines a balloon as; 'a *balloon is a lighter-than-air aircraft that is not engine driven, and that sustains flight through the use of either gas buoyancy or an airborne heater*'[42].

4.4.1 BLOON – 'Zero2infinity'

Zero2Infinity are a new company developing a 'near space' balloon (BLOON) with the goal of attaining a height of 36km for their 2-3 hour flight. The vehicle will be able to accommodate 4 passengers and 2 pilots.

4.4.2 BLOON Technology

The BLOON technology strategy is to base the approach on existing technology but have a novel integrated solution and flight profile up to an altitude of 40km.

[41] http://en.wikipedia.org/wiki/Joseph_Kittinger
[42] http://www.faa-aircraft-certification.com/faa-definitions.html

Figure 67: BLOON's Sail

The sail is basically a balloon filled with inert helium. It bears the whole system through the atmosphere, with no fuel or propellant, no noise and no discomfort.

Figure 68: BLOON's 'Pod', Descent Aerofoil, Chain and Landing Sub-system

The chain links the pod and the sail. It also contains the necessary communication and localization systems and BLOON's emergency landing system.

The Pod will serve as the passenger (and pilot) cabin whereby the splendours of the Earth will be viewed in a comfortable 'shirt-sleeved' environment.

The Landing System shown in Figure 68 is deployed in the descent phase. The system is comprised of two segments:

- *Textile-based decelerators: ensures a quiet descent, directing the pod to its chosen landing site.*
- *Inflatable absorbing systems: enables the attenuation of forces to make the landing as comfortable as possible*

4.4.3 BLOON Safety

BLOON will have a robust safety-by-design philosophy which will adopt three levels of redundancy. Additionally there is no rocket-power involved that the technology and therefore this could be considered >90% safer (meaning that 80-90% of the spacecraft risk is due to the rocket propulsion system and 9% of the risk is during re-entry).

- *Tier 1 – Balloon based on known design and filled with Inert Helium*
- *Tier 2 – Textile-based decelerators*
- *Tier 3 – Emergency Landing System*

Additionally the pod will have two pilots and is designed on a submarine/ISS philosophy whereby the occupants do not have to wear pressure suits because of the exacting load factors that BLOON will design to (exceeding those of SoAs or RLVs). Additionally the pod will be under lower and more predictable quasi-static loads unlike SoAs or RLVs.

A progressive test strategy is also envisaged with early testing conducted in Sweden's Esrange Space Centre. Then it is envisaged that first commercial flights will be over low-populated areas until more reliability data is gathered.

BLOON's technology and safety strategy appear sound and based on known technology (for the atmospheric balloon); however the technology for the human capsule or 'pod' is novel and will be challenging to get certified. Standard balloon certification routes can be followed but additional rules and guidelines will need to be applied and these will have to be rationalised. These aspects will be covered in the following sections.

4.4.4 Review of Current Information

4.4.4.1 Hot Air Balloons

Hot Air Balloons are flown regularly and appear to have a reasonable safety record and this is backed up by the UK CAA's CAP 780 [102]:

> *"There were 27 reportable accidents involving UK public transport balloons in the period 1998- 2007. None of these reportable accidents was fatal, although there were 10 serious injuries and 41 minor injuries. There were no serious incidents involving UK public transport balloons in the period 1998-2007. There were 100 occurrences, of which two were considered to be high severity. No utilisation data are available for UK public transport balloon operations; therefore rates of accident, serious incident and occurrence cannot be calculated."*

An American website has published accident rates for balloons though only include a two-year period:

Year	# of Accidents	# of Fatalities	Flight Hours	Accidents per 100,000 Hours
1997	17	2	48,700	34.90
1996	22	2	68,000	32.37
Total	39	4	116,700	33.62

Table 25: Hot Air Balloon Accident Statistics

Table 25 above shows the accident rate for hot air balloons as 33.62 per 116,700 flying hours[43] which equates to an accident rate of 2.9e-04 per flying hour. As a comparison General Aviation accident rates are currently 7 in 100,000[44] which equates to $7x10^{-5}$ per flying hour or $0.7x10^{-4}$ per flying hour (with an implicit target of 1 in 10,000). Although the comparison is made here the reality is that balloons fly lower (mainly) and slower and hence the number of deaths is low; therefore is the comparison meaningful?

CS-31HB – Certification Specification for Hot Air Balloons

[43] https://www.facworld.com/FACWORLD.nsf/Doc/Hotairballoon
[44] http://www.avweb.com/avwebflash/news/ntsb_preliminary_crash_statistics_rate_accident_fatal_202309-1.html

Hot Air Balloons are certified against CS31HB.25 [103] and have guidelines published in AMC 31HB.25 (b) [contained in Book 2 of the CS31-HB]. The only relevant safety requirement appears to be related to the design load factor which is 1.5 except for the following aspect:

A factor of safety of 5 or more must be used in envelope design. A reduced factor of 2 or more may be used if it is shown that the selected factor will preclude failure due to creep or instantaneous rupture from lack of rip stoppers. The selected factor must be applied to the more critical of the maximum operating pressure or envelope stress. (See AMC 31HB.25 (b))

The CS and AMC contain design and construction requirements and operating limitations but these do not reflect any safety objectives.

Additionally, the AMC covers 'equipment' on board and states:

> *The correct functioning should not be impaired by operational circumstances such as icing, heavy rain, high humidity or low and high temperatures. The equipment, systems, and installations should be designed to prevent hazards to the balloon in the event of a probable malfunction or failure of that equipment.*
>
> *When ATC equipment and/or positioning lights as possibly required by operational rules are installed, it should be shown that the electrical system is such that the operation of this equipment is not adversely affected by operational circumstances.*

Arguably equipment should have their own safety case and the hazards should be analysed accordingly and a probability of failure stated which should meet standard aviation requirements (and safety objectives).

As the CS did not contain any safety objective requirements other relevant documents were reviewed.

CAP494 – British Civil Airworthiness Requirements

CAP494 [104] contains similar design, construction and operating requirements as the CS-31HB but in addition contains basic safety objectives i.e. '*the envelope shall not distort in a manner likely to lead to a hazardous loss of lift or control'*, however the document does not categorise the safety objectives.

4.4.4.2 Transport Airships

A review of Transport Airship Requirements (TARs) was undertaken to determine whether there were any suitable cross-over from airships to hot air balloons (in particular to assist in determining effective criteria for 'near space' balloons).

TAR 1309 – Equipment, Systems and Installations

The airship requirements have explicit safety objectives as per the aviation requirements:

> *(1) Any catastrophic failure condition*
> *(i) is extremely improbable; and*
> *(ii) does not result from a single failure; and*
> *(2) Any hazardous failure condition is extremely remote; and*
> *(3) Any major failure condition is remote.*

TAR 571 – General

The structure must be designed, as far as practicable, to avoid points of stress concentration where variable stresses above the fatigue limit are likely to occur in normal service. An evaluation of the strength, detail design, and fabrication must show that catastrophic failure due to fatigue, corrosion, or accidental damage, will be avoided throughout the operational life of the airship.

A probability approach may be used in these latter assessments, substantiating that catastrophic failure is extremely improbable.

TAR 581 – Lightning Protection

The airship must be protected against catastrophic effects from lightning.

TAR 671 – Control Systems (General) – if applicable

> *(1) Any single failure not shown to be extremely improbable, excluding jamming, (for example, disconnection or failure of mechanical elements, or structural failure of hydraulic components, such as actuators, control spool housing, and valves).*
>
> *(2) Any combination of failures not shown to be extremely improbable, excluding jamming (for example dual electrical or hydraulic system failures, or any single failure in combination with any probable hydraulic or electrical failure).*
>
> *(3) Any jam in a control position normally encountered during cargo loading/unloading, passenger boarding/un-boarding, take-off, climb, cruise, normal turns, and descent and landing unless the jam is shown to be extremely improbable or can be alleviated. A runaway of a flight control to an adverse position and jam must be accounted for if such runaway and subsequent jamming is not extremely improbable.*

TAR 803 – Emergency Evacuation

If the occurrence of fire hazard for the passenger and crew compartments in crash landings cannot be considered extremely improbable, it must be shown that the maximum passengers capacity, including the number of crew members required by the operating rules for which certification is requested, can be evacuated from the airship to the ground under simulated emergency conditions within 90 seconds.

4.4.4.3 BLOON's Equipment

Parafoils

The second descent phase for BLOON involves the deployment of a 'parafoil' which is essentially a non-rigid textile aerofoil as depicted in Figure 68. The parafoil was developed by Domina Jalbert[45] in 1964 and he envisaged its use in airborne delivery platforms or for the recovery of space equipment. Due to its aerofoil shape, the parafoil has greater steer-ability, allows for increased glide range and allows for greater control (flare for instance) in particular for landing. As opposed to a round parachute, the parafoil is considered a 'square' parachute (actually rectangular) and this feature, along with the ability to deflect one end or the other in order to turn (or deflect both for a flare manoeuvre) is the main differentiator in its selection for airborne delivery platforms and hence the BLOON project.

[45] http://en.wikipedia.org/wiki/Parafoil

NASA has used parafoils on a number of programs including the X-38 and the Genesis program with varying success. The X-38 program was a crew return vehicle that required a parafoil to slow the landing speed from 250 knots vehicle design speed to 40 knots; the parafoil's ability to flare was a major feature in its selection, along with the steer-ability. The NASA report [105] detailed 300 successful tests of a subscale parafoil (wing area 750ft^2) and 33 tests with full scale parafoils (5000 ft^2 and 7500 ft^2); though these tests were from aircraft at various altitudes and using an extractor parachute which then deployed the drogue prior to deploying the parafoil. The requirements for the tests did not include safety objectives but were noted as:

- *Repeatable, low dynamic, on-heading openings*
- *Space-rated materials*
- *High design factors*
- *Increased failure tolerance*
- *Parachute weight and volume restrictions*
- *Landing impact velocity and acceleration limits.*

The X-38 program was subsequently cancelled however the US Department of Defence then took over the program and developed the parafoil with a guidance system for use in the delivery of cargo loads. No statistics are available for the equipment.

A parafoil was also used on NASA's Genesis project which cited a 100% success rate during the test phase of the parafoil. However after the Sample Return Capsule had re-entered Earth's atmosphere the 'Drogue' parachute failed to deploy and hence the parafoil was not deployed; this resulted in the Capsule being destroyed. The Mishap Investigation Board's Report [106] found that the root cause was failure of the 'G-Switch' which should have activated and deployed the drogue 'chute' in order to deploy the parafoil. As the load was a space capsule then the resultant consequence of the accident was catastrophic loss of the equipment. Figure 69 details the Genesis parafoil and details the suspension lines and risers.

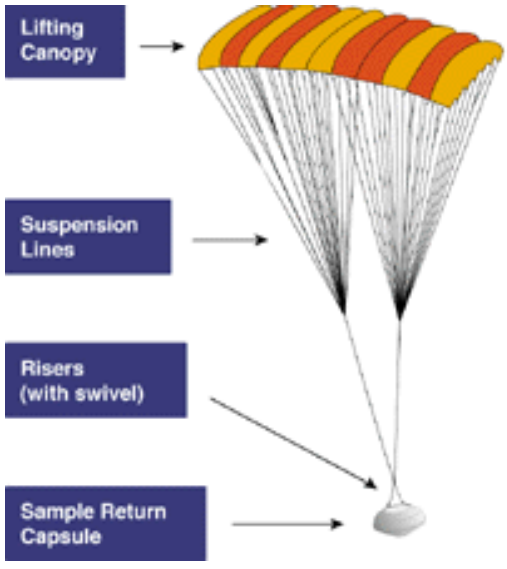


Figure 69: NASA Spacecraft 'GENESIS' Sample Return Capsule with Parafoil deployed

Military airborne delivery equipment (ADE) tends to have one or more round parachutes depending on the size of the load. For a heavier load (or equivalent to the Near-Space Pod or X-38 program) two or three parachutes are used compared to the single parafoil.

Indeed military ADE technology has developed since the X-38 program and a good analogy is the evolution of the Joint Precision Airdrop System (JPADS) program. JPADS combines the Army's Precision and Extended Glide Airdrop System (PEGASYS) program with the USAF's Precision Airdrop System (PADS) program to meet joint requirements for precision airdrop and wants to satisfy four identified principal needs/"gaps" in the joint airdrop functional area; increased ground accuracy, standoff delivery, increased air carrier survivability, and improved effectiveness/assessment feedback regarding airdrop mission operations. JPADS has four projected weight increments linked to a common mission planner and/or aircraft components: JPADS-2K for up to 2,200lbs; JPADS-10K – 10,000 lbs.; JPADS-30K for up to 30,000lbs; and JPADS-60K for up to 60,000 lbs.

These systems require incrementally larger canopies and in comparison the X-38 would fit into the JPADS-30K category whereas the BLOON system fits into the JPADS-10K category and therefore has lower technological challenges. A similar system is the Smart Parafoil Autonomous Delivery System (SPADES) which is in the '2K' weight range which aims to be certified against Dutch military airworthiness requirements[46].

The author has knowledge of square and round parachutes due to working on the safety aspects for these systems and the following are considered typical hazards:

- Parachute fails to deploy: due to the following causes;
  - Extractor failure (drogue parachute failure)
  - Static line not attached
  - Parachute canopy cells ripped
  - Air Starvation – parachutes side-by-side often have this
  - Contamination – water/icing
- Premature Parachute disconnect: due to the following causes;
  - Mechanical disconnect failure
  - Air Starvation (as the load then senses 'relief' and the mechanical disconnect releases the parachute
- Obstruction in the Drop Zone (inherent hazard); in this instance the parafoil is steer-able so obstructions should not be an issue

The above hazards would apply to BLOON's parafoil system and there will be many more hazards to analyse and to manage with appropriate mitigation (see 4.4.9 below regarding Functional Hazard Analysis); indeed in the case of the 'GENESIS' parachute malfunction the BLOON profile is more benign but the hazard analysis will need to be conducted for 'drogue not deployed' (for the parafoil).

The Pod ECLSS

BLOON's pod is designed for two pilots and four passengers and is planned to fly to an altitude of 40km with the total flight lasting two hours. As opposed to hot air balloons or even transport air balloons the BLOON pod will require an environmental conditioning and life support system (ECLSS). This will be a closed-loop system and must comply with basic requirements such as those contained in FAA 460.11 [71] as follows:

> *(a) An operator must provide atmospheric conditions adequate to sustain life and consciousness for all inhabited areas within a vehicle. The operator or flight crew must*

46 http://www.dutchspace.nl/uploadedFiles/Business_Fields/Defense/SPADES/SPADES%20Smart%20Parafoil%20Autonomous%20Delivery%20System%201000%20Mk2%20(2,200%20lbs).pdf

monitor and control the following atmospheric conditions in the inhabited areas or demonstrate through the license or permit process that an alternate means provides an equivalent level of safety—

(1) Composition of the atmosphere, which includes oxygen and carbon dioxide, and any revitalization;

(2) Pressure, temperature and humidity;

(3) Contaminants that include particulates and any harmful or hazardous concentrations of gases, or vapours; and

(4) Ventilation and circulation.

(b) An operator must provide an adequate redundant or secondary oxygen supply for the flight crew.

(c) An operator must

(1) Provide a redundant means of preventing cabin depressurization; or

(2) Prevent incapacitation of any of the flight crew in the event of loss of cabin pressure.

In addition to the closed-loop system, BLOON's design of the pod's interior incorporates three pressure-isolated zones that have two functions concerning privacy (for intimate flights) and primarily for safety; in the event of slow depressurisation the crew and passengers can move to one of the isolated zones as safety mitigation.

The pod also employs an emergency system which can provide an extra mass flow inlet in order to compensate for the exiting air as a result of depressurization thereby maintaining the internal pressure within safe values during the time required for the emergency procedure; the emergency procedure will consist of taking the passengers to one of the three pressure isolated modules in the pod and then initiating an emergency descent using textile-based decelerators or even a free fall to a safe height.

Avionics Equipment

Although the Pod will not employ Complex Programmable Equipment (CPE) such as for essential flight requirements in Suborbital Aircraft any equipment used in the system such as automatic flight control system for the parafoil guidance system, navigational equipment or communications equipment must be safe and hence follow the relevant certification requirements. BLOON's equipment is stated to be a transponder, radar reflector and Global Positioning System.

4.4.4.4 BLOON's Flight Profile

The Ascent Phase

Helium Lift-Off

The balloon starts the ascent due to the lifting force of helium. The helium expands, thus getting colder, as the balloon goes up in the troposphere at an average ascent speed of 5 m/s. This ascent rate quickly drops to 2 m/s at the tropopause since the helium's temperature is colder than the atmospheric temperature. A ballast release is then required to increase the ascent rate. This operation shall be repeated as many times as necessary. The ballasting system is a simple hatch, which is remotely controlled and can be opened and closed to release small lead or glass spheres. This system will be controlled from the inside of the cabin.

The Descent Phase

Venting & Free-fall

The initial part of the descent involves opening the venting valves which are located at the top of the balloon and are remotely controlled. At cruise altitude the solar radiation is very high and it makes the helium temperature increase thus over-expanding the balloon. The valves will remain open about 40-50 minutes (depending on the helium temperature) so that the balloon slowly starts descending (V<1m/s). Additional venting operations will be necessary to reach a descent rate of 3-4m/s. In the event the descent rate exceeds a limit value (i.e. 4m/s) it can be reduced by releasing additional ballast.

BLOON has the ability to include a 'free-fall' phase between the vent phase and deployment of the parafoil. This could provide a 30-second microgravity phase prior to deployment of the drogue parachute which then deploys the parafoil.

4.4.4.5 BLOON Operator Considerations

Other issues that BLOON may wish to consider include:

- Wind – this is a major factor affecting the safe flight of a Hot Air Balloon and also the parafoil. Limitations will have to be in place regarding wind-speed limits
- Icing – At altitude this may be a factor and certain control systems may have to have anti-ice capabilities
- Lightning - This is an 'extremely improbable' event but one that must be considered in terms of mitigation strategies; bonding of equipment and static wicks are design features and also procedural controls will be to check the weather and avoid the chance of lightning
- Bird-strike – The windows should be designed to withstand a large bird impact at altitude. As this event may be 'occasional' then the design strength plays a major factor in mitigating the issue. Additionally this may play a major factor in determining whether or not to have pressure suits or emergency oxygen available i.e. in the case of a cracked window due bird-strike and the pod is subject to de-compression. Finally the operator procedures should include pre-flight planning in terms of weather and also obtaining information on bird migration and nesting so that the areas can be avoided.
- Loose Articles – The windows should also be shatter-proof against passenger's loose articles in particular in the descent phase (post sail release and prior to the parafoil deployment i.e. in the microgravity phase
- Flight Corridor – The flight profile is up to 40km and for two hours duration and therefore a flight corridor will need to be established with a NOTAM in place with the ATM system. Additionally;
  - The NOTAM will provide sufficient mitigation to exclude other air vehicles. This must be for a 'corridor' of specified altitude, length and width
  - The operator should engage with ATC to derive 'windows of opportunity' for BLOON whereby the air traffic is 'light' within or near the corridor; this can reduce the exposure of other air traffic thereby reducing the exposure to a mid-air collision. Initially for the test phase BLOON will fly from Esrange Space Centre (Kiruna, Sweden); Esrange has launched many high-altitude balloons and sounding rockets and therefore Air Traffic should not present an issue. However when flying commercially a flight corridor will be required.
- Pilot's License and Medical – Standard requirements for Hot Air Balloons could apply with perhaps more stringent elements due to the extreme altitude and technology and additional training for specialist medical equipment
- Pax requirements – Passengers should have Medical Certificates from their general Practitioners, however it is advisable to have specific questions relating to the flight
- Safety equipment – the following safety equipment should be provided;

- Fire fighting appliances will be required in the pod
- Medical Equipment - Additionally as the pod is a more serene flight than a SoA and with more room, medical first aid equipment could be carried
- Pilot and Passenger seat restraints will be required
- Protection against sun glare
- Personal Parachutes (see 4.4.4.4 above and 4.4.8 below)
- Emergency Oxygen supply
- Pressure suits for test flights and early flights in order to acquire enough confidence with the system; indeed BLOON already plan to conduct their first flights using pressure suits similar to the ones used by Russian MIG pilots like the VKK-6M or the VMSK-4.

4.4.5 Certification Route

BLOON could arguably apply for certification through the Spanish Civil Aviation Authorities (Directorate General of Civil Aviation) as per normal hot air balloons using CS-31B. Clearly the main difference is the 'near space' altitude and flight profile which would require integration with the Spanish (and European) ATM System with appropriate NOTAMs. BLOON could also engage EASA for specialist advice and possible certification if outside the competence of the Spanish Authorities. Special Conditions will apply (Special Conditions will also apply to Suborbital Aircraft for example) and these will be discussed with the authority as part of the certification of the vehicle; some of these SCs are detailed in Table 29 below such as Environmental Conditioning and Life Support Systems (ECLSS).

Recommendation: It is recommended that BLOON engage EASA's assistance in determining suitable safety criteria for their near space system. This recommendation is carried forward to 6.3.

4.4.6 Proposed Safety Criteria for 'Near Space' Balloons

There appears to be little quantitative requirements in terms of certifying balloons and air ships and therefore there are certainly no existing criteria applicable to the BLOON project. So is the answer to apply an Equivalent Level of Safety (ELOS) approach in which BLOON provides evidence of equivalence to the existing CS-31B in the form of design analysis and operating procedures and supplementing specific additional requirements (such as relevant TARs or Special Conditions identified by the designer and regulator)?

In terms of safety criteria, should the BLOON project have a safety target approach, a failure condition safety objective approach or a simplified safety requirement approach? With a simplistic hot air balloon system, statistics showing a failure rate of 2.9e-04 per flying hour (as detailed in 4.4.4 above); can we derive a safety target for a more complex system using this accident rate as a baseline? It is considered that the hot air balloon accident rate sample is too small (only over a two-year period) and so more rationale is required in the derivation of such a target. The BLOON vehicle will be a low usage product (lower than hot air balloons) and one could argue that a safety target of 1 in 10,000 ($1x10^{-4}$) catastrophic events could be achievable. Additional reasoning is that the BLOON is not like an aircraft/SoA/RLV in that there are not 100 catastrophic failure conditions (probably 10 catastrophic events) and so the achievement of the safety target is not unrealistic; whereas in the case of SoA it will be challenging to meet a catastrophic safety target of 1x10-4 per flying hour because of the rocket propulsion system reliability.

It could also be argued that qualitative criteria will suffice as that is what hot air balloons are currently certified to. The following is based on the analysis for the SoA but simplified using qualitative descriptions for likelihood (probability) classifications and using standard severity classifications:

Likelihood (preferred option to meet CS)	Probability (optional internal company classifications to assist in determining whether internal safety target is met)	Qualitative Description
Frequent	$>1x10^{-2}$	Likely to occur often in the life of the system
Probable	10^{-2} to 10^{-3}	Likely to occur several times in the life of the system
Occasional	10^{-3} to 10^{-4}	Likely to occur sometime in the life of the system
Remote	10^{-4} to 10^{-5}	Remote Likelihood of occurring in the life of the system
Improbable	10^{-5} to 10^{-6}	Extremely unlikely to occur in the life of the system
Extremely Improbable	$<10^{-6}$	So unlikely, it can be assumed occurrence may not be experienced in the life of the system

Table 26: Proposed Likelihood Classification for BLOON

Description & Category	**Actual or Potential Occurrence**	**Effect To People**			**Effect to Asset**	**Effect to Environment**
		1st Parties	**2nd Parties**	**3rd Parties**		
Catastrophic	Accident	Multiple 1st Party deaths	Multiple 2nd Party deaths	Single 3rd Party death	Loss of spacecraft	Extreme widespread environmental damage
Hazardous	Serious Incident - Asset or Accident (people death/injury)	Single 1st Party death Physical distress or excessive workload impairs ability to perform tasks	Single 2nd Party death	Multiple Serious injuries 3rd Party (requires hospital treatment more than 2 days)	Severe damage to spacecraft Large reduction in Functional capabilities or safety margins	Severe environmental damage
Major	Major Incident	Multiple Serious injuries/ illnesses to 1st Parties (requires hospital treatment more than 2 days) Physical discomfort or a significant increase in workload	Multiple Serious injuries/ illnesses to 2nd Parties (requires hospital treatment more than 2 days) Physical discomfort	Single Serious injury to 3rd Party (requires hospital treatment more than 2 days)	Major damage to spacecraft Significant reduction in functional capabilities or safety margins	Major environmental damage
Minor	Minor Incident	Minor injuries/illnesses to 1st Parties (requires first aid and/or hospital treatment for less than 2 days) Slight increase in workload	Minor injuries/illnesses to 2nd Parties (requires first aid and/or hospital treatment for less than 2 days)	Minor injury to 3rd Parties (requires first aid and/or hospital treatment for less than 2 days)	Minor damage to spacecraft Slight reduction in functional capabilities or safety margins	Minor environmental damage
Negligible	Occurrence without safety effect	Inconvenience	Inconvenience (requires assistance and is reportable)	Single Minor injury to 3rd Party	Less than Minor damage	Less than minor environmental damage

Table 27: Proposed Severity Classifications for BLOON

The following Risk Matrix (based on the *SATURN SAFETY MODEL*) is proposed for BLOON. The rationale is that the matrix can be used with the qualitative approach but also with the (internal company) quantitative approach; the rationale for the later approach is to determine whether the evidence can be gained to meet a safety target (of 1 in 10,000 catastrophic failures for instance). The purpose of this would be to demonstrate that the ELOS requirements of CS-31B and associated Special Conditions had been met and indeed exceeded. Using this top-down approach for an emerging and novel system would be a pragmatic approach. In terms of individual safety critical systems we can then derive that the designer must be able to demonstrate the 10 catastrophic failure conditions meets the circa 1 in 100,000 per flying hours failure rate; this should be achievable for the known sub-systems such as the parafoil, balloon and helium sub-system. The pod is the notable exception and the designer would have to argue excessive safety margins (per submarine/ISS design margins) in terms of providing evidence that the load factor has been met with a lot of reserve and that the operating profile is benign (as opposed to high-g SoA/RLVs); along with BLOON's emergency depressurisation strategy. Also by having a safety target approach (with implicit safety objectives) then arguably the 10 catastrophic failure conditions could be in the catastrophic 'C' cell (for 1 in 100,000) and still meet the safety target of 1 in 10,000.

The Risk Matrix categories accord with the Transport Airship Requirements in the absence of specific criteria from CS-31B:

(1) Any catastrophic failure condition
  (i) is extremely improbable; and
  (ii) does not result from a single failure; and
(2) Any hazardous failure condition is extremely remote; and
(3) Any major failure condition is remote.

	Severity (Safety Event)				
Likelihood/Probability	Catastrophic (Accident)	Critical/ Hazardous (Serious Incident)	Major (Major Incident)	Minor (Minor Incident)	Negligible
Frequent $> 10^{-2}$	**A**	**A**	**A**	**B**	**C**
Probable 10^{-2} to 10^{-3}	**A**	**A**	**B**	**C**	**D**
Occasional 10^{-3} to 10^{-4}	**A**	**B**	**C**	**D**	**D**
Remote 10^{-4} to 10^{-5}	**B**	**C**	**D**	**D**	**D**
Extremely Remote 10^{-5} to 10^{-6}	**C**	**D**	**D**	**D**	**D**
Extremely Improbable $<10^{-6}$	**D**	**D**	**D**	**D**	**D**

Table 28: Proposed Risk Matrix for BLOON

An alternate method of determining a loss rate is to use the 'abort rate' methodology as detailed in section 2.2.6.1 (for a winged spacecraft low test rate strategy) whereby 2 abort events were required for a vehicle loss and this then had an assumption of only 50% of accidents resulting in fatalities. Their analysis detailed that '*this implies a vehicle loss rate of 1 in 20,000 which equates to a loss of life probability of 1 in 40,000 and therefore they claim that their initial estimates suggest they are more than one hundred times 'safer' than the Space Shuttle'.*

4.4.7 Proposed Technological Requirements

From the above discussions and general review of suborbital technical requirements in 2.3.8.2 the following additional safety-based Technical Requirements could be applicable to BLOON:

ID	Requirement	Source	Rationale
1	CS-31B standard requirements (that are applicable)	CS31-B/ AMC to CS31-B	EASA and National Aviation Authorities will understand the CS for Hot Air Balloons and then BLOON can engage with the Authorities' Subject Matter Expert to derive Special Conditions (and safety targets/objectives). Of particular importance (among others that are applicable) is the means to indicate the maximum envelope skin temperature or maximum internal air temperature during operation.
2	ECLSS requirements	FAA 460.11	CS31-B concerns 'baskets' that are not pressurised clearly. The pod will be a closed-loop system and must conform to standards
3	Pod Structural Load	TAR 571	In that 'An evaluation of the strength, detail design, and fabrication must show that catastrophic failure due to fatigue, corrosion, or accidental damage, will be avoided throughout the operational life of the [pod]'
4	Emergency Oxygen System	FAA 460.11	In addition to the closed-loop system in case of depressurisation a redundant system should be employed i.e. the use of individual emergency oxygen or other suitable design feature (such as the BLOON three pressure isolated modules and extra mass inlet flow)
5	Smoke Detection & Fire Suppression System	EASA 851-865 FAA 460.13	Fire suppression must be compatible with a closed-loop system. Fan blowers may be required to ensure smoke can be detected throughout the flight i.e. during possible microgravity periods
6	Doors	EASA 783	No untimely opening of doors but to have the means of opening quickly in the event of an emergency
7	Bird-strike impact requirements (from outside)	EASA 775	windows should be designed to withstand a large bird impact at altitude
8	Loose article impact requirements (from inside)	EASA 775	windows should also be shatter-proof against passenger's loose articles in particular in the descent phase (post sail release and prior to the parafoil deployment i.e. in the microgravity phase
9	Lightning Protection	TAR 581	The airship must be protected against catastrophic effects from lightning
10	Weather Limits	Non-specific	(in addition to Balloon requirements) i.e. Wind for the parafoil and Icing for the landing and emergency systems
11	Seats & Restraints	EASA 785	Hot Air balloons have handles for passenger restraint whereas the pod will have seats fitted – these (and the restraints) must meet EASA requirements
12	Emergency Evacuation	TAR 807 EASA 803, 805-813	On top of the 90-second requirement on the ground, BLOON should consider in-flight bail-out in emergency situations and by the use of parachutes
13	Personal Parachute Requirements	Civil/ Military standards	Only applicable if used as an emergency measure (recommended)
14	Parafoil requirements	Parafoil Standards Institute of America	PSIA and other relevant standards for parafoils
15	Extractor (drogue) parachute	Military/NASA	Extractor parachute should have an ELOS of the

ID	Requirement	Source	Rationale
	requirements	standards	GENESIS system and can therefore be argued to be better as the re-entry is not from orbit
16	Medical Equipment	Non-specific	as the pod is a more serene flight than a SoA and with more room, medical first aid equipment could be carried
17	Passenger information signs	EASA 791	Required as part of certification
18	Validation & Verification programme	FAA 460.17	This should be standard within the design lifecycle for the equipment and also include safety V&V
19	Software Safety	DO-178-B	Depending on equipment employed – may not be applicable
20	Complex Hardware	DO-254	Depending on equipment employed – may not be applicable

Table 29: Proposed Additional Technical Requirements for BLOON

4.4.8 Proposed Additional Safety Mitigation

BLOON's strategy of a balloon-style near space ride is clearly safer in terms of not being subject to RPS issues and high g-force issues and current designs have sound mitigation built in. From the above discussions additional safety mitigation could be implemented and strengthen the safety case.

- Survivability Measures
  - Personal Parachutes – in the event of an envelope failure, arguably the parafoil can be deployed (via the drogue chute). In the unlikely event of either a drogue chute failure or a parafoil failure (either to deploy or to be able to provide control) then what is the last line of safety for the passengers and crew? The landing system (inflatable absorbing system) is really only to assist in normal landings and with hard landings, so would not be of any use in the case of high altitude parafoil failures. An option is to provide passengers with personal parachutes. These are presently issued to people on experience flights in gliders and for high-performance flights such as in the 'Extra 300' flights[47]. However although these are an additional level of emergency mitigation it also brings challenges in terms of training and 'bail-out' hazards. However it is here that the designer could employ the safety technique of Cost Benefit Analysis (CBA) to determine that the costs versus the benefit gained.
  - Personal Capsules – Capsules or escape pods could be designed that incorporate their own parachute system. Again the designer could employ the CBA technique to determine that the costs of designing such a system would be grossly disproportionate to the benefit gained.

4.4.9 Proposed Safety Management Strategy

As the BLOON project is more complex than a hot air balloon it is recommended that a safety case strategy is adopted and backed up by a robust Safety Management System; especially as BLOON state that '*safety is our first priority'*. This should start with a Safety Management Plan for the project accompanied by a simplified System Safety Program Plan for the designers.

In terms of safety assessment and to assist in providing certification evidence for this more complex system it would be prudent to demonstrate that hazards have been identified and their likelihood's established and that residual risks have been classified and are being managed to as low as reasonably practicable.

[47] http://www.extrabatics.com/Thrillrides.aspx

The *SATURN SAFETY MODEL* detailed in the thesis would be appropriate for BLOON's safety analysis.

The Functional Block Diagram (FBD) approach should be used and the exemplar FBD (Figure 41) is reproduced below in Figure 70 with those functions that are not applicable 'crossed-out'; the purpose of this is to demonstrate that the functions do need to be analysed but also that there are far fewer relevant functions. Additionally some of the functions needed to be changed to represent BLOON's design such as replacing 'provide engine motive thrust' with 'provide helium-assisted lift' and 'replacing 'provide control of aircraft roll attitude' with 'provide directional control of parafoil' as detailed below:

- To Aviate (fly)
  - To provide helium-assisted lift'
  - To provide control of the platform (in the air)
  - To provide directional control
  - To provide control of the platform (on the ground)
  - To provide structural integrity
  - To provide visibility
- To Navigate
  - To provide awareness of platform state (in terms of altitude, heading and (vertical) speed)
  - To provide platform current position and flight path data
- To Communicate
  - To provide external visual clues (meaning to communicate visually)
  - To provide external communications
- To Transport (including containment)
  - To provide habitable areas
  - To provide crew seats/restraint
  - To provide passenger seat/restraint
  - To provide normal ingress/egress
  - To provide emergency egress
  - To provide ability to contain helium systems
  - To provide ability to contain aircraft equipment
  - To provide ability to release containment of helium
- To Display platform conditions
  - To detect and warn of platform conditions
  - To manage equipment and systems operation

These remaining and retitled functions would then be analysed in a platform level FHA. Following this the sub-system FHAs would be undertaken along with Occupational Health Hazard Analysis, Operating & Support Hazard Analysis and Zonal Hazard Analysis.

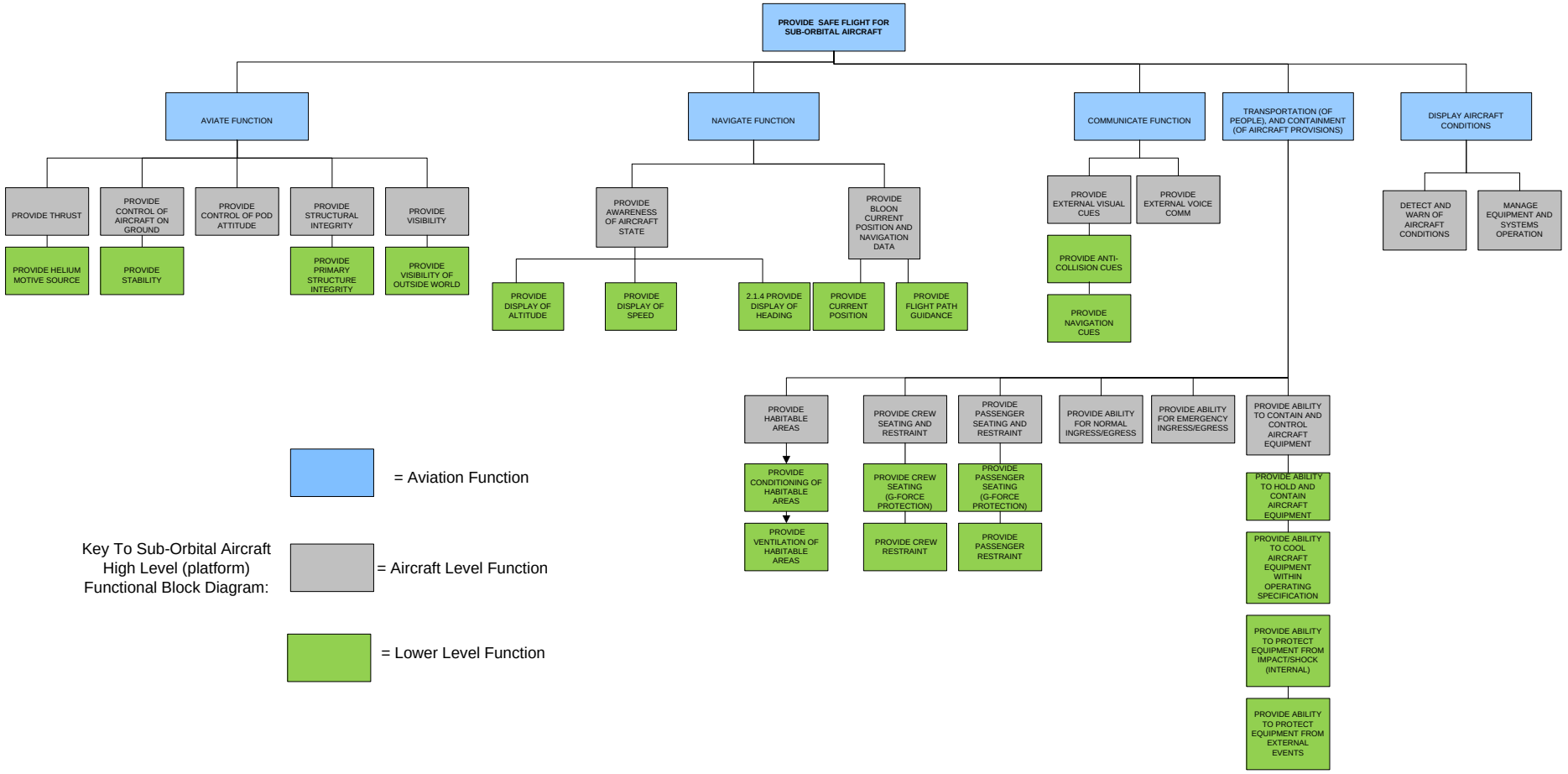


Figure 70: Functional Block Diagram representing the Suborbital Aircraft functions and those aspects not relevant (crossed out) to BLOON

4.4.10 BLOON REVIEW CONCLUSION

The BLOON project presents an interesting and unique design and ‘near space’ operating profile and this appears to have less risk than the current SoA/RLV spacecraft designs with Rocket Propulsion System hazards and high-g-forces. The current design philosophy and safety strategy appears robust at this early phase and is based on a three-tier safety philosophy.

The review concludes that there are no specific certification criteria for the design apart from the hot air balloon criteria (CS-31B); this does not cover all of the BLOON aspects and does not detail quantitative safety objectives. The certification could be undertaken with the Spanish Authorities in the normal manner for hot air balloons with the addition of Special Conditions such as for the ECLSS and other operating issues such as design requirements for bird-strike impact with the windows. BLOON could employ an Equivalent Level of Safety approach to meet the requirements of the CS and Special Conditions and indeed can be industry fore-runners in setting safety standards and safety objectives. EASA could also assist in this or with the whole certification of BLOON.

In terms of Safety Management the BLOON project states that ‘safety is our first priority’ and this should be backed up with the implementation of a robust Safety Management System and employing a safety case strategy due to the additional complexities of the system (over normal hot air balloons). A Safety Manager should be an essential part of the team from the early phases of design progression and be responsible directly to the Chief Executive Officer as well as the Program Engineer. Additionally an Independent Safety Auditor could be employed though an Independent Technical Evaluator may provide sufficient oversight for the authorities.

CHAPTER FIVE – Validation of Research

5.1. FINDINGS

The thesis has uncovered various levels and types of safety best practice and guidelines for organizations to follow and has found that in the main these are being followed to the best of people's competences. However it was interesting to find that the metrics used in determining the safety level of an aircraft (and spacecraft) **stopped** at the design organisations boundary i.e. the infamous $1x10^{-9}$ per flight hour for a catastrophic failure condition for aircraft. This value was derived from analysis of historic accident rates which were 1 in a million ($1x10^{-6}$ per flight hour). This was then broken down into 10% of accidents due to safety critical system failures and with 100 arbitrary safety critical systems thus resulting in $1x10^{-9}$ per flight hour. In the suborbital safety domain the Federal Aviation Administration Office of Commercial Space Transportation (FAA-AST) have provided regulations and safety guidance material in the form of Advisory Circulars and other generic guidance and it was found that the safety criterion within has not been rationalised (per the aviation criterion mentioned above) and that this is not helping the industry[48]. Furthermore it was found that although some of the generic guidance was based on aviation and NASA best practice this was not necessarily relevant for the nascent suborbital domain; an example of this that the FAA-AST is focused on protecting the 'public' i.e. 3rd parties and has not been concerned with protecting the flight crew and space flight participants (SFP). The reason for this is that the boundaries of the FAA-AST are considered too expansive in that 'commercial spaceflight' covers not only the suborbital domain but also the orbital industry; here is the main problem in that the regulations and guidelines are really for a Launch License to orbit and these have been modified slightly for the suborbital domain. Clearly with designs such as Virgin Galactic's air-launched aircraft-based vehicle which flies within a remote and excluded corridor (vertically as well as horizontally excluded) then the risk to the public will be very low indeed as compared to a vertical orbital-bound vehicle that will at some point overfly a populated area; both in terms of people on the ground and aircraft in the air.

It was found that aircraft operators use risk profiling from their Flight Operations Quality Assurance (FOQA) process and some airline safety managers did not even use a hazard log. Therefore the airworthiness or design risks presented by 100 catastrophic failure conditions were not taken forward in an accident sequence whereby operator procedures, training and operating limitations should be used as controls to prevent an accident.

This lack of contiguous safety approach provided an interesting challenge to develop such a model for the suborbital industry and then possibly for the aviation industry.

The review also found that there were no such regulations or guidelines for suborbital operations in Europe and this provided an opportunity to establish these with EASA and therefore assist in influencing the European-based suborbital designers and operators.

5.2. SIGNIFICANCE OF FINDINGS

The research found that the FAA-AST safety criterion was extremely poor and that they were employing a launch license approach; the significance of this meant that the FAA-AST methodology would not be appropriate within a European regulatory framework.

[48] Based on the author's discussions and work for Virgin Galactic and from the views of the industry noted at space conferences (2nd IAA and 4th IAASS)

Another of the major findings of the research was that the safety analysis was not contiguous from the designer to the operator and therefore the operator was not fully aware of the risks of the aircraft (spacecraft). This is clearly presented within a case study of the Air France AF447 disaster whereby the designer knew about the design issues with the pitot-tubes and instigated a Service Bulletin for all operators to change them; Air France were still flying ten days later without changing procedures, training or introducing limitations and subsequently the aircraft and all on board were lost. The *SATURN SAFETY MODEL* shows the failings and had the operator employed proactive safety management and in particular using an explicit model then the people would still be alive today. This is the same for the Space Shuttle's Challenger and Columbia and these also were subject to a case study using the new model.

5.3. FUTURE RESEARCH

The thesis highlighted various issues that were outside the scope of the main objectives and these were summarised with recommendations for future research. Most of the future research recommendations can be direct actions for the International Association for the Advancement of Space Safety (IAASS) new Suborbital Space Safety Technical Committee (SSS TC) which the author initiated and is the Chair of; hence these are on the agenda to be resolved as near-to-medium objectives.

Further research is required with EASA to substantiate the SoA Policy (goal-based regulatory safety case) due to the timeframe of European Commission's decision to continue with the task.

5.4. INTERPRETATION OF RESULTS

The results of the thesis show that a new safety model is required for the emerging suborbital domain and that this could also be applicable for the aviation domain.

The results of the EASA Suborbital Aircraft Policy safety argument shows that the regulations and guidelines of the existing EASA framework can accommodate SoA requirements; but this requires the addition of Special Conditions. The evidence was backed up by using FAA-AST regulations and guidelines as references where applicable however there were instances when these were considered not robust enough for EASA SoA certification requirements or for EASA SoA guidelines; examples being that the FAA-AST only require a Class II Aerospace Medical Certificate for flight crew whereas EASA now require a Class I and the FAA-AST only consider the 'public' in terms of Expected Casualty (Ec) and use a launch license approach whereas EASA intend to certify the SoA and therefore also consider the pilots and SFPs.

5.5. SIGNIFICANCE OF RESULTS

It is considered that the results are significant in that this thesis has highlighted a gap in the safety methodology being employed today by designers and operators in that they are not employing a contiguous approach to safety; rather that they are doing things very well in their own area of responsibility and this can have drastically negative effects as demonstrated in the Air France Flight AF447 case study. The results have shown that by using a contiguous safety approach and by employing a formal safety model then the safety manager (responsible person) and the operator's Chief Executive Officer (accountable person) will know their Accident Risks and Total System Risks and will therefore be able to manage these by reducing the risks so far as is reasonably practicable i.e. being able to demonstrate this by means of cost benefit analysis or decision analysis and to justify this within their safety statements for each risk.

In terms of the EASA SoA Policy it was expected that the case for safety could be argued however the significant aspect is that EASA are not competent to certify the 'space segment' (as they have stated all along) and this has not been addressed by the industry thus far. This is a significant issue that needs to be resolved by the suborbital community and this is within the remit of the IAASS Suborbital Space Safety Technical Committee and this is recommended as such in Chapter Six.

5.6. AUTHOR'S VALIDATION OF THE 'THESIS CASE'

5.6.1 Personal Validation

The structure of this Thesis was governed by the Goal Structured Notation methodology and the Goals were presented in Section 1.3. To validate the '**Top Goal'** (that the research strategy meets the criteria for award of a PhD) it was necessary to examine the evidence provided to support the sub-goals (G1 to G4) i.e. was the literature and industry review effective and were innovative methodologies and guidance provided as a result of the review. Finally it was important that the thesis was effectively validated.

(G1): The review of spaceflight-related literature and industry standards ensures a thorough understanding of personal spaceflight issues; G1 is supported by Evidence of sufficient literature review (E1.1) and Evidence of Personal Spaceflight Industry review (E1.2):

> Evidence E1.1: The review of spaceflight safety literature focused on existing orbital spaceflight aspects in order to determine whether any lessons could be identified that would carry forward to the suborbital industry. Here it was useful to identify not only the infamous disasters but also the 'near misses' in order to gain a better understanding of the risks involved in spaceflight. The second part of the literature review concentrated on the safety tools and techniques available that may be appropriate for use in the suborbital vehicle design and operations. This was important because rather than just accept 'the norm' in civil aviation and governmental-led space programs the review provided a chance to analyse the standards and guidelines in order to determine which would be suitable for the suborbital domain. Here it was found that there was a 'disconnect' between the design system safety analysis and the operator safety risk management. This meant that operators were basing their risk assessments qualitatively in a bespoke manner and therefore could not possibly comprehend the risks presented to the aircraft either by severity type or indeed the total risk presented by the aircraft.
>
> The evidence is substantiated in sections 2.1 and 2.2.
>
> Evidence E1.2: The personal spaceflight industry review focused on the nascent suborbital domain and as the industry is yet to get off the ground this provided a useful opportunity to determine whether the regulations and guidance material were acceptable or not. The FAA-AST is the leading regulatory body as the fore-runners in the industry are based in America. The reviews concentrated on the FAA-AST safety-related documents and although some were found reasonable and based on good practice others were found to be more applicable to the orbital domain rather than the suborbital domain. Here it was found that the FAA-AST is covering 'commercial spaceflight' which includes both orbital and suborbital; the author contends that the two fields are distinct enough to warrant their own regulations and guidelines (though it is acknowledged that some common areas exist and so these could be rationalised as such). Within Europe the review highlighted that EASA have no such regulations or guidance material and so this presented an opportunity to assist in providing rationalised safety management information within a new framework. EASA had provided a

stance that they believed that suborbital aircraft (SoA) could be dealt with in an existing European certification framework but EASA were not authorised by the European Commission to do so as yet. Additionally the author had attended many spaceflight conferences and established many contacts within the domain and was able to review the industry presentations to gauge whether a safety culture was emerging and also whether the correct legal authority had been established to govern the suborbital flights.

The evidence is substantiated in section 2.3.

(G2): The Gap Analysis is comprehensive in order to meet the aims and objectives; G2 is supported by Evidence (E2.1) Authors Papers and Evidence (E2.2) Authors Gap Analysis.

Evidence E2.1: The review included identifying the 'current state' of the industry and analysed whether gaps existed such that possible methodologies and guidelines could be developed to assist in deriving a 'future state'. Throughout the period of the research a number of papers were authored and presented at the space-related conferences in order to promote the gaps and important aspects within the suborbital industry.

The evidence is substantiated at Appendices 8 – 12.

Evidence E2.2: The gap analysis was a contiguous effort through the review and therefore this evidence is implicitly linked with E1.1 and E1.2.

(G3): The proposed methodologies and guidelines are innovative and appropriate for the identified disciplines; G3 is supported by Evidence (E3.1) EASA SoA Policy GSN (Rules & Guidelines), (E3.2) Suborbital Spaceflight Training (&Medical) Analysis, (E3.3) Operator Analysis and Evidence, (E3.4) Spaceport Analysis, (E3.5) Synthesis of Emerging technologies) and (E3.6) New Safety Model.

Evidence E3.1: The task to support EASA in deriving a SoA Policy and guidance material provided an opportunity to influence the suborbital domain in terms of safety criteria (for certification aspects) and safety management considerations (as supplemental considerations for guidance material). The author assisted in the initial Pre-Regulatory Impact Assessment which is a process that determines whether the risk and effort is within EASA's remit and competence. Then the author continued with the EASA team looking at the baseline Policy structure. The author then produced a goal-based argument for the Policy (that needed to be instantiated) and also continued with more detailed safety management activities for later when deriving guidance material for designers and operators. The current status is that the European Commission has yet to make the decision to continue with the task despite a number of potential designers/operators requesting assistance from EASA in certifying their SoA.

The evidence is substantiated at 3.2, 3.3 and APPENDIX 5 - Suborbital Aircraft Policy – Goal Structuring Notation.

Evidence 3.2: The suborbital spaceflight training and medical review highlighted that the FAA-AST approach was too 'flexible' and although in Europe it is not the intent to stifle the industry the regulations and guidelines must be sufficiently robust in order to minimise accidents or incidents. The author's knowledge coupled with industry expert opinion provided guidelines that were appropriate for the nascent industry.

The evidence is substantiated at section 3.6.

Evidence E3.3: Although the planned SoA operators such as Virgin Galactic and Rocketplane were not able to assist in the thesis Zero2Infinity were able to assist in providing information from which to analyse their design and operations. The 'near space' balloon and pod system was an interesting model to analyse from a safety management perspective and to determine whether the operator would be receptive from the guidance provided.

The evidence is substantiated at section 4.4.

Evidence 3.4: The Spaceport analysis was conducted by synthesis only. This was achieved by reviewing the FAA-AST Environmental Requirements for Spaceports, reviewing the Launch Site safety documents and also reviewing the standard airport requirements. This enabled a cohesive set of requirements to be formed for a Spaceport Safety Management System.

The evidence is substantiated at section 3.5.

Evidence 3.5: There are various emerging technologies within the suborbital domain and these are discussed as to the potential issues and risks presented by the systems. In particular rocket propulsion systems and emergency systems (such as ballistic recovery systems, spacesuits and parachutes) are discussed. In the later the case for spacesuits is explored further and a safety tool is used to assist in the decision as to whether to employ spacesuits or not. The tool used is Cost Benefit Analysis (CBA) which stems from the UK Health and Safety Executive's ALARP principle. This can also be backed up by sensitivity analysis where the parameters in the CBA calculation can be altered. Finally a 'decision' analysis is a formal way of stating that a control measure is introduced (such as a spacesuit) for socio-political reasons even if the CBA calculation suggests that the cost is disproportionate to the benefit gained.

The evidence is substantiated at section 4.1, 4.2 and 4.3.

Evidence E3.6: The review highlighted a lack of contiguous safety analysis in the aviation and space domains (from designer to operator) despite there being good practice guidelines at the designer level and the operator level. Ultimately this meant that the operator is unaware of the risks presented by the aircraft and was unaware of the effect of operator control failures; this was proved by the use of case studies (Air France AF447 disaster and the Space Shuttle disasters). This provided an opportunity to close the gap and determine whether a contiguous safety model was possible. The author identified that a platform level hazard existed (a 'Key (Platform) Hazard') which formed the missing link in the contiguous safety model. This is then linked to specific ICAO-based accidents (and/or Safety Significant Events) at the operator safety risk analysis and finally a feedback method is employed to the base events of the designer analysis.

The evidence is substantiated at section 3.4.

(G4): The validation process is effective in ensuring the Thesis has met the Top Goal; G4 is supported by Evidence (E4.1) Authors Findings, Evidence (E4.2) Authors Discussions, Authors Recommendations (E4.3) and also Validation by EASA Evidence (E4.1.1), Operator Validation Evidence (E4.1.2)

Evidence E4.1, E4.2 and E4.3 are substantiated in sections 5.1 through to 5.5.

Evidence E4.1.1: EASA validation is substantiated at section 5.7.1

Evidence E4.1.2: Operator validation (Zero2Infinity). The evidence is substantiated at section 5.7.2.

5.7. VALIDATION BY REGULATORY BODIES & INDUSTRY

5.7.1 EASA Validation

The following provides the validation from EASA's perspective. The relevant Chapters 2.4.8 (review), 3.3 and 3.4 (with Appendix 4) cover the analysis concerning the EASA Suborbital Aircraft Policy and guidelines. As stated within the relevant chapters the EASA main SoA task has yet to be authorised from the EC and the research has focused on the preliminary phases of suitability and applicability. Additionally Chapter 3.4 provides 'supplemental considerations' which is the author's more explicit analysis that may be used by EASA in preparing their guidelines for the European-based suborbital industry.

> *Andy Quinn's thesis is a comprehensive synthesis, as well as a projective reflexion on the current and future main challenges faced by the personal spaceflight industry in terms of safety. His work may be profitably used as a baseline of discussions in future cooperative research works. However, although being in charge of the safety of aviation in Europe, i.e. for the safety of European citizens with respect to operation of aircraft, including Sub-orbital Aircraft in the European airspace, at the present stage, EASA is not officially involved in any rulemaking or certification task for SoA. Therefore, the above validation reflects only a personal opinion, based on the professional experience of the reviewer both as ESA Astronaut Safety Manager and EASA SoA Coordinator. Also, it should be noted that discussions on the safety objective to apply to SoA are still not conclusive, although a consensus amongst EASA experts was aiming at a level similar to the one of Class III Commuters, as indicated in AMC 23.1309.*
>
> Jean Bruno Marciacq
> EASA SoA Coordinator

5.7.2 zero2infintiy Validation

The following provides the validation from a designer/operator's perspective. The relevant Chapter 4.4 covers the analysis of the BLOON project based on research undertaken for this thesis.

> *As the first sustainable experiential aerospace company, zero2infinity's mission is to elevate our planetary consciousness. zero2infinity's maiden vehicle, BLOON, has been designed from day-1 to provide the 21st century traveller with the most life-enriching and meaningful journey beyond the blue skies into the blackness of Space. So we are fortunate to live in a time when a new industry is developing. The general public is about to enlarge its sphere of accessibility above commercial aircraft routes to ever higher spaces. More than anything else, safety is the enabler. It's the make or break criterion for the success of the industry. Andy's work on the topic is comprehensive, ground-breaking and will long be a reference. The analysis shows some points to think about and I think that the Functional Block Diagram is particularly complete and interesting. Also the section 4.4.7 (Proposed Technological Requirements) could be very useful to analyse the safety issues concerning particular parts or subsystems.*
>
> Jose Miguel Bermudez Miquel (on behalf of Jose Mariano Lopez Urdiales, CEO)
> Product Developer, zero2infinity (BLOON Project)

CHAPTER SIX – Conclusions & Recommendations

6.1. CONLUSIONS ON SAFETY

The review provided the author with an interesting task of examining existing safety management system methodologies within the aviation and space domains and to back this up with academic reviews in order to piece the puzzle together. It is concluded that in general all aspects of both industries are 'doing their bit for safety'. However the various organizational component parts are doing their bit in accordance with their way of doing things and herein lay the problem; there is not a contiguous safety effort.

Previously at NASA[49] designers, HMI, safety and operators did not come together until required at certain milestones and finally at the last stages of the development. Also the disparate organizations had resulted in a poor safety culture and hence management were cited as contributors in the Space Shuttle disasters. Today in NASA we have designers talking to safety and we have designers talking to HMI, but we do not have designers talking to HMI **and** safety[50]. What are the safety objectives that design organisations have to meet and what does this mean in terms of catastrophic safety targets i.e. does NASA have one? In particular for the ISS the focus is on 'product safety' and there are stringent requirements backed up by effective operating procedures; but none of this appears to be managed at the total system level and thus it could be argued that the Total System Risk is unknown. The Space Shuttle safety is based on the ISS standards and requirements and once again do they know the Total System Risk. As the Shuttle Program ends and NASA discuss future commercial programs they are talking about 'certification' and safety of the crew and passengers; finally progress in the right direction (as opposed to just being concerned about the 'public' safety).

Within aviation we have airbus meeting certification standards with their safety analysis and operators (such as Air France) doing their operator safety risk management; however they use different metrics and therefore the operators are assuming a lot from their design colleagues and have not fully understood the accident sequence and their role in ensuring safety of the aircraft. The thesis uses the AF447 disaster in proving the systemic disconnect and proving that a contiguous safety model approach could have averted the accident.

The nascent suborbital industry is led by fore-runners in America with poor guidelines on safety because the FAA-AST regulatory and guideline scope is for 'commercial' spaceflight and this includes orbital and suborbital. These two domains are literally miles apart and also miles apart in terms of the approach required to provide safe assurance of the vehicles and therefore the flight crew and space flight participants. The suborbital safety effort within Europe will focus on an existing EASA regulatory framework for aircraft certification and this is a different approach to the FAA-AST and their launch license approach which is biased towards the orbital vehicles i.e. vertical launch and with an equatorial-based flight trajectory and hence this will be over a populated area at some point. Currently these fore-runners have provided some interesting design solutions for their experimental phase but it is assumed that these will then be employed for operations; the problem here is that there are good safety features but the designs have not fully explored the survivability/crashworthiness aspects that would have been part of the systems safety analysis at the beginning of a project. It is known that one of these leading companies did not even have a safety manager until recently and they

[49] The author's view on NASA presentations and how they have progressed and improved their processes. 4th IAASS, Huntsville, May 2010
[50] As per footnote 48

have been designing the vehicle for many years now (and involving the operator from the beginning); hence there is concern from the general space industry[51] about the safety culture and safety management of these 'newcomers'. This is not surprising due to the lack of rationalised safety guidelines; after all these are not companies who have a long established history in aircraft or spacecraft design/manufacturing for the commercial market.

6.2. OTHER CONLUSIONS

The thesis provided an opportunity to provide a synthesis on emerging technologies within the suborbital domain and also to provide a synthesis on the safety management at a Spaceport.

It is concluded that the fore-runners in the suborbital domain are experimental-based designers and these are providing some unique and disparate models which appear exciting and novel. However to win the second space race they appear to have missed a couple of steps in the design lifecycle and gone for the engineering solution-driven approach. An example is that in the event of a Loss of Control (for instance in the 'space segment' i.e. the RCS has failed and they are still upside down and unable to recover due aerodynamic forces) then an accident control would be to have a Ballistic Recovery System (BRS). This realisation would only have been a resulting conclusion from a formal Functional Hazard Analysis at the beginning of the program. This could also have been backed up with an optimisation approach whereby a Cost Benefit Analysis would prove whether the cost of introducing a BRS proved beneficial (in terms of reducing the severity [consequence]); even in the US where Space Flight Participants will be required to sign a 'waiver' not to sue and that they know the risks involved, the lawyers (in the event of a Loss of Control accident) will no doubt look for what was mitigation was reasonably afforded their clients – in this instance the operators will probably lose the argument.

Spaceports are just glorified airports – or are they? With some RLV/SoA designs such as EADS-Astrium's rocket-plane and indeed Rocketplane's own design, the vehicles take-off and can land under normal engine power and therefore should be able to take-off from an airport. However in this case, the airport would have to get additional certification in terms of storing and handling of rocket propellants and therefore may take the name of a Spaceport/Airport in any case. Other designs such as XCOR (rocket initiated on the runway) or Armadillo Aerospace's vertical RLV will not be able to launch from a normal airport and hence must be certified as a Spaceport. The addition of rocket propellant and noise issues are governed in the US by the FAA-AST Environmental Guidelines and therefore this thesis has been able to derive safety requirements based on those guidelines with the addition of airport guidelines and additional knowledge gained from the industry. It is considered that Spaceports can be certified and can operate safely by incorporating a Safety Management System early on in their design and throughout their operation.

6.3. RECOMMENDATIONS ON SAFETY

6.3.1 New Safety Model

The review highlighted gaps in the current safety management methods in terms of a lack of contiguous safety approach between designers and operators. There is effective guidelines for designers in order to achieve an airworthy aircraft (spacecraft) and there is some guidelines for operators to identify and manage their hazards and risks; however these are not joined up and therefore there is a danger that the operator is unaware of his overall (total system) risk - or even

[51] '*Concern about the safety of these newcomers'* was stated at the 4th IAASS conference in Huntsville, Alabama, May 2010.

individual or severity class risks. The *SATURN SAFETY MODEL* proposed in Chapter 3.4 presents a contiguous safety model that was validated by using case studies both in the aviation domain (Air France flight AF447) and in the space domain (Space Shuttles Challenger & Columbia).

Recommendation: It is recommended that the safety model is presented to the suborbital industry, authorities and agencies for consideration.

Recommendation: It is recommended that the safety model is presented to the aviation industry, authorities and agencies for consideration.

6.3.2 Continuation of EASA Task

At the time of thesis submission EASA were awaiting approval from the EC to continue with the Suborbital Aircraft Policy. In the meantime the author continued the analysis and goal-based regulatory safety case.

Recommendation: It is recommended that EASA continue to substantiate the SoA Policy (goal-based regulatory safety case) when approval is received from the EC to continue the task.

6.3.3 EASA to Derive Safety Criteria for Near Space Balloons

The BLOON project is a near space balloon and although CS31-B could apply in part, Special Conditions will be required for the BLOON system. Additionally there are no formal safety targets or safety objectives and it is recommended that BLOON engages with EASA to derive a safety target as a minimum.

Recommendation: It is recommended that BLOON engage EASA's assistance in determining suitable safety criteria for their near space system.

6.4. OTHER RECOMMENDATIONS FOR FUTURE STUDY BY THE IAASS SSS TC

Further work considerations for the IAASS Suborbital Space Safety Technical Committee include:

6.4.1 Suborbital Space Segment Safety

Within Europe EASA is competent to certify SoA up to but not including the space segment of the flight. The FAA-AST has no delineation in terms of a Launch License 'environment' (domain) and they are also not certifying RLVs therefore they do not have the issue. The safety of SoA within the space segment requires discussion mainly in terms of the legal aspects i.e. who is competent to accept responsibility (for safety and of course liability). The design of the vehicles will strive to provide for safe flight i.e. ECLSS, Reaction Control Systems and in terms of the operator, the requirements to ensure Space Flight Participants are secured in their seats for the descent and hence this is not the real issue for EASA because the descent is within the remit of EASA.

The argument is whether to adopt a Space Law regime or an Air Law regime and the outcome of this debate will then realise whom the regulators are and as to whether the vehicles (RLV or SoA) should be licensed or certified.

Recommendation: It is recommended that the IAASS SSS TC undertake the analysis and provide the best practice/guidelines to the appropriate authorities.

6.4.2 Vertical Launch Criteria

Vertical Launch System in the European Arena: Spaceport Sweden are considering Vertical Launches as well as trying to get Virgin Galactic to operate from there. Vertical launches are considerably more

hazardous than horizontal or air-launch systems due to the potential for explosion on rocket initiation. Flight Safety abort systems are required (more so that for horizontal systems arguably) because an occurrence could result in a Fire/Explosion and the aim is to try and prevent the death of not only those on board but also the support staff (2nd party) and spectators (3rd party). Further work is required in this area to determine the criteria to which safety should be demonstrated. Using the logarithmic methodology from the American Standards approach [84] one could simply add another level of severity and probability to that of horizontal/air-launch.

Recommendation: It is recommended that the IAASS SSS TC undertake analysis in relation to vertical launch criteria within the suborbital domain.

6.4.3 Abort Rate Criteria

There are difficulties in establishing loss rates for new equipment and section 2.2.6 discussed an 'abort rate' that was calculated from a loss rate. The analysis should be further investigated and in particular this may be useful for the suborbital vertical launch/vertical landing vehicles such as Armadillo Aerospace.

Recommendation: It is recommended that the IAASS SSS TC reviews the 'abort rate' methodology provided by Reaction Engines Ltd (for their orbital based design 'SKYLON') at the 2nd IAA conference in order to determine its merit for use in the suborbital domain.

6.4.4 Safety Model Hazard Log

The Safety Model detailed in Section 3.4 culminated in the development of a prototype Hazard Log that accommodates the methodology of the Safety Model. As opposed to Design Organisation hazard logs and separate Operator Safety Risk management tools (risk profiles and hazard logs), the Saturn SMART Hazard Log provides an integrated approach that is User-friendly and provides relevant information and reports to enable Duty-Holders to make appropriate Safety-related decisions; mainly concerning Risk but also concerning design changes.

The Saturn SMART Hazard Log has been developed to a prototype stage in order to gauge the viability of the tool. This must now be developed further to include a web-based Server.

Recommendation: It is recommended that the Hazard Log tool is developed further with a mainstream software provider.

6.4.5 Organisational Safety Risks

The *SATURN SAFETY MODEL* in highlighted a need to include the organisational and support activities as part of the safety analysis. The Operating & Support Hazard Analysis (OSHA) is a good technique that can uncover many organisational and human-related issues that should be considered (in particular by the Operator).

6.4.6 FRR Flight Risk Assessment

The FRR Flight Risk Assessment is a tool to assist in the decision-making for suborbital operations. It should be validated and reviewed to include further aspects to consider prior to flight in order to ensure that all relevant flight-related risks have been assessed.

Recommendation: It is recommended that the IAASS SSS TC undertake analysis based on the findings in 3.4.12 in relation to Flight Readiness Review (FRR) Flight Risk Assessments.

6.4.7 Suborbital Medical Standards

There are currently no detailed and rationalised medical standards for Suborbital Space Flights. The following recommendations should be carried out to provide a more robust and rationalised approach to medical standards for suborbital flights.

Recommendation: It is recommended that the IAASS SSS TC undertake analysis based on the findings in 3.6 in relation to Flight Crew & Space Flight Participant Medical & Protective Equipment Standards.

6.4.8 Suborbital Training Standards

There are currently no detailed and rationalised training standards for Suborbital Flights. The following recommendations should be carried out to provide a more robust and rationalised approach to training for suborbital flights.

Recommendation: It is recommended that the IAASS SSS TC undertake analysis based on the findings in 2.3.6 and above centrifuge and anti-g suit proposals

Recommendation: It is recommended that the IAASS SSS TC undertake analysis based on the findings in 2.3.3 and above simulator proposals

Recommendation: It is recommended that the IAASS SSS TC undertake analysis based on the findings in 2.3.6 and above altitude training proposals

Recommendation: It is recommended that the IAASS SSS TC undertake analysis based on the findings in 2.3.6 in regards to Space Flight Participants

6.4.9 Occurrence Reporting

The existing Air Safety Reporting scheme requires reviewing to include suborbital flight phases and aspects as applicable.

Recommendation: It is recommended that the IAASS TC undertake a review of the Air Safety Reports (mishap reports) with regards to suborbital domain requirements.

Acronyms/Abbreviations

Acronym/ Abbreviation	Meaning
AC	Advisory Circular
ACARS	Automatic Communication Addressing and Reporting System
ADE	Airborne Delivery Equipment
ALARP	As Low As Reasonably Practicable
AMC	Acceptable Means of Compliance
ANR	Active Noise Reduction
AOC	Air Operator Certificate
ARMS	Aviation Risk Management Solution
ARP	Aerospace Recommended Practices
ASIC	Application Specific Integrated Circuits
AsMA	Aerospace Medical Association Working Group
ASR	Air Safety Report
ATC	Air Traffic Control
ATM	Air Traffic Management
ATO	Abort to Orbit
BRS	Ballistic Recovery System
CAA	Civil Aviation Authority
CAP	Civil Aviation Publication
CEO	Chief Executive Officer
CEP	Communications Ear Plug
CFR	Code of Federal Regulations
CHS	Commercial Human-Rated Systems
CLSAA	Commercial Space Launch Amendments Act
COPUOUS	Committee on the Peaceful Uses of Outer Space
CPE	Complex Programmable Equipment
CPLD	Complex Programmable Logic Devices
CS	Certification Specification
DAL	Design Assurance Level
Def-Stan	Defence Standard
DO	Design Organisation
EA	Environmental Assessment
EASA	European Aviation Safety Agency
EC	European Commission
Ec	Expected Casualty
ECLSS	Environmental Conditioning and Life Support System
ELOS	Equivalent Level of Safety
ETA	Event Tree Analysis
EU	European Union
EVA	Extra Vehicular Activity
FAA	Federal Aviation Administration
FAA-AST	Federal Aviation Administration Office of Commercial Space Transportation
FAA-AVS	Federal Aviation Administration Aviation Safety
FAI	Fédération Aéronautique Internationale
FBD	Functional Block Diagram
FC	Failure Condition
FCL	Flight Crew Licensing
FHA	Functional Hazard Analysis
FMECA	Failure Modes Effects and Criticality Analysis

FOQA	Flight Operations Quality Assurance
FPGA	Field Programmable Gate Arrays
FRAM	Functional Resonance Accident Model
FRR	Flight Readiness Review
FSS/FTS	Flight Safety System/Flight Termination System
ft	Feet
FTA	Fault Tree Analysis
GA	General Aviation
GAIN	Global Aviation Information Network
GAMAB	Globalement Au Moins Aussi Bon
G-LOC	G-Induced Loss of Consciousness
GSN	Goal Structuring Notation
HF	Human Factors
HMI/HME	Human Machine Integration/Engineering
HRI	Hazard Risk Indices
HSE	Health & Safety Executive
IAA	International Academy of Aeronautics
IAASS	International Association for the Advancement of Space Safety
IFR	Instrument Flight Rules
IIP	Instantaneous Impact Point
IMC	Instrument Meteorological Conditions
ISS	International Space Station
ISSF	International Space Safety Federation
ISU	International Space University
ICAO	International Civil Aviation Organisation
JPADS	Joint Precision Airborne Delivery System
JSSG	Joint Services Specification Guide
LOX	Liquid Oxygen
MoD	Ministry of Defence
N_2O	Nitrous Oxide
NAS	National Airspace
NASA	National Aerospace and Space Administration
NOTAM	Notification to Airman
NPA	Notice of Proposed Amendment
NPRM	Notice of Proposed Rulemaking
OHHA	Occupational Health Hazard Analysis
OSHA	Operating and Support Hazard Analysis
PADS	Precision Airborne Delivery System
PEGASYS	Precision and Extended Glide Airdrop System
PFH	Per Flight Hour
PHL	Preliminary Hazard List
PPPY	Per Person Per Year
PRE	Preliminary Risk Estimation
PSSA	Preliminary System Safety Assessment
RIA	Regulatory Impact Assessment
RLV	Reusable Launch Vehicle
RPS	Rocket Propulsion System
RTC	Restricted Type Certificate
SB	Service Bulletin
SC	Safety Case
SC	Special Conditions
SCR	Safety Case Report

S-FME(C)A	Software Failure Modes Effects (and Criticality) Analysis
SFP	Space Flight Participant
SHA	System Hazard Analysis (same as SSA- System Safety Analysis)
SIL	Safety Integrity Level
SMS	Safety Management System
SoA	Suborbital Aircraft
SRK	Skills-Rule-Knowledge (based errors)
SS1/SS2	Space Ship 1 and 2
SSE	Safety Significant Event
SSS	Suborbital Space Safety
SSWG	Software Safety Working Group
STAMP	Systems-Theoretic Accident Model and Processes
SWG	Safety Working Group
TAL	Transatlantic Landing
TC	Technical Committee
TNA	Training Needs Analysis
TTS	Thrust Termination System
ULT	Upper Level of Tolerability
UN	United Nations
V&V	Validation & Verification
VFR	Visual Flight Rules
VMC	Visual Meteorological Conditions
VTOL	Vertical Take-Off and Landing
WK2	White Knight 2
ZHA	Zonal Hazard Analysis

References & Bibliography

1: URL, X-Prize. ***http://www.xprize.org/.***

2: URL, Bigelow. ***http://www.bigelowaerospace.com/.***

3: Futron Corporation. ***Suborbital Space Tourism Demand Revisited*****, August 24 2006.**

4: Ve. Ziliotto. ***Relevance of the Futron/Zogby survey conclusions to the current space tourism*****, Acta Astronautica (2009), doi:10.1016/j.actaastro.2009.08.027**

5: URL, FAA-AST. http://www.faa.gov/about/office_org/headquarters_offices/ast/.

6: Federal Aviation Administration (FAA). Guide to Reusable Launch and Re-entry Vehicle Reliability Analysis, Version 1.0, April 2005, page 7.

7: Vaughan, D. ***The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA.*** **Chicago; University of Chicago Press Ltd, 1996.**

8: Columbia Accident Investigation Board Report, 2003

9: Charles Haddon-Cave QC, ***The Nimrod Review*****, 28th October 2009**

10: Van Pelton M, Space Tourism: Adventures in Earth Orbit and Beyond, Praxis Publishing, 2005

11: URL, NASA. http://www.hq.nasa.gov/library/pathfinders/accidents.htm

12: URL, Roscosmos, ***http://www.federalspace.ry/php?id=10&year=0***

13: Scaled Composites, Update Details to Accident, 1 August 2008

14: URL, Rocket and Space Technology. http*://www.braeunig.us/space/index_top.htm***

15: Kemp K, ***Destination Space*****, Virgin Books Limited, 2007**

16: International Association for the Advancement in Space Safety, Independent Space Safety Board, ***Space Safety Standard – Commercial Manned Spacecraft*****, Revision B, dated Aug 2006**

17: International Association for the Advancement of Space Safety, Independent Space Safety Board, ***Space Safety Standard for Commercial Human-Rated Systems*****, March 2010**

18: Federal Aviation Administration (FAA). Hazard Analyses for the Launch or Re-Entry of Reusable Suborbital Rocket Under an Experimental Permit. s.l. : FAA, 2007. AC:437.55-1.

19: URL, OALD. ***Oxford Advanced Learner's Dictionary.*** **s.l. : Oxford University Press, 2009.**

20: Cullen, Lord. ***The Public Enquiry into the Piper Alpha Disaster.*** **s.l. : HMSO, 1990.**

21: Federal Aviation Administration (FAA) Code of Federal Regulations, Title 14, Chapter III, Part 401, Sub-Part A (General)

22: Federal Aviation Administration (FAA) Code of Federal Regulations, Title 14, Chapter III, Part 417, Launch Safety

23: HSE. Railway Safety Cases - Railway (Safety Case) Regulations1994 - Guidance on Regulations. s.l. : Health and Safety Executive, 1994.

24: ICAO. ***ICAO 9859 - Safety Management Manual.*** **s.l. : International Civil Aviation Organization, 2009.**

25: UK Civil Aviation Authority, ***Safety Management Systems - Guidance to Organisations.*** **s.l. : UK CAA, 2008.**

26: Federal Aviation Administration (FAA). ***AC 150/5200-37, Introduction to SMS for Airport Operators.*** **s.l. : FAA, 2007.**

27: URL, EuroControl. ***http://www.skybrary.aero/index.php/Safety_Management.*** **s.l. : EuroControl SKYbrary, 2009.**

28: MoD, UK. ***Defence-Standard 00-56, Issue 4.*** **2007.**

29: Federal Aviation Administration (FAA), System Safety Handbook, Chapter 15: *Operational Risk Management*, December 30, 2000

30: Shelton C P, Human Interface/Human Error, Carnegie Mellon University, 18-849b Dependable Embedded Systems, Spring 1999

31: Chappelow J W, *The Risk of Human Error*; Data Collection, Collation and Quantification, Centre for Human Sciences, DERA Farnborough

32: UK, Ministry of Defence, Defence-Standard 00-56, Issue 2, 1996

33: Federal Aviation Administration (FAA), AC120-92, *Introduction to Safety Management Systems for Air Operators*, 22 June 2006

34: ARMS Working Group, Operational Risk Assessment, 2007-2010

35: Global Aviation Information Network, Operator's Flight Safety Handbook, Issue 2, December 2001

36: Leverson N, A New Accident Model for Engineering Safer Systems, Massachusetts Institute of Technology

37: Dijkstra A, Resilience Engineering and Safety Management Systems in Aviation, KLM Royal Dutch Airlines

38: Hollnagel E, Modelling of failures: From chains to coincidences, Presentation, 2007

39: SAE International, Aerospace Recommended Practice, *Certification Considerations for Highly Integrated or Complex Aircraft*, ARP 4754, 1996

40: UK Ministry of Defence, Acquisition Operating Framework, *Occupational health Hazard Analysis Guidelines*

41: Federal Aviation Administration (FAA), FAA-DI-SAFT-105, Operating & Support Hazard Analysis

42: RTCA Incorporated, DO-178B, Software Considerations in Airborne Systems and Equipment Certification

43: National Aeronautics And Space Administration, Software Safety Guidebook, NASA-GB-8719.13, March 31 2004

44: RTCA Incorporated, DO-254, DESIGN ASSURANCE GUIDANCE FOR AIRBORNE ELECTRONIC HARDWARE

45: IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems

46: Federal Aviation Administration, Aviation Rulemaking Advisory Committee, Task 2 – System Design and Analysis Harmonization and Technology Update, 24 May 1996

47: European Aviation Safety Agency. CS-23, Certification Specification for Normal, Utility, Aerobatic and Commuter Category Aeroplanes, 2003

48: European Aviation Safety Agency. CS-25, Certification Specification for Large Aeroplanes, 2007

49: ICAO. The Convention on International Civil Aviation, Annex 8, Airworthiness of Aircraft

50: UK Ministry of Defence, Joint Service Publication 553, Issue 2

51: Federal Aviation Administration (FAA). Advisory Circular AC 25-1309-1A, *Systems Design and Analysis*, dated 21 June 1988

52: US Department of Defence, Joint Service Specification Guide, *Air Vehicle*, 22 October 2002

53: US Department of Defence, MIL-STD-882D, Standard Practice for System Safety, Change 1, October 2008

54: International Academy of Aeronautics, 2nd IAA Conference Proceedings', 30 May – 1 June 2011

55: UK Health & Safety Executive; URL, http://www.hse.gov.uk/risk/theory/alarpglance.htm

56: UK Health & Safety Executive, Reducing Risks Protecting People, 2001

57: UK Civil Aviation Authority, CAP 719, Fundamental Human Factors Concepts, 15 February 2002

58: Reason J, Managing the Risks of Organizational Accidents, Ashgate, 2004

59: European Union, Council Regulation (EEC) No 3922/91, EU-OPS, 20 August 2008

60: Federal Aviation Administration (FAA) Code of Federal Regulations, Title 14, Chapter III, Sub-Chapter A, Part 400, Basis and Scope of Regulations

61: Federal Aviation Administration (FAA-AST) Advisory Circular, AC 431-35-2A, *Reusable Launch and Re-entry Vehicle System Safety Process,* July 20 2005

62: Federal Aviation Administration (FAA-AST), *Guide to Reusable Launch Vehicle Safety Validation and Verification Planning, Version 1,* September 2003

63: American Institute of Aeronautics and Astronautics- Federal Aviation Administration (FAA-AST), *Guide* to the identification of Safety Critical Hardware Items for *Reusable Launch Vehicle Developers*, 1 May 2005

64: Federal Aviation Administration (FAA-AST), *Guide to Reusable Launch and Re-entry Vehicle Software and Computing System Safety, Version 1,* July 20063

65: Quinn C A, *Commercial Space Travel: Safety Management of the Customer,* Master's Thesis, 2006

66: Federal Aviation Administration (FAA-AST), Draft Guidelines for Commercial Suborbital Reusable Launch Vehicle Operations with Space Flight Participants, Feb 11 2005

67: Federal Aviation Administration (FAA – AST), Draft Guidelines for Commercial Suborbital Reusable Launch Vehicle Operations with Flight Crews, Feb 11 2005

68: Mosunmoluwa S A, Emergency Medicine for Human Suborbital Spaceflight, March 2008

69: Aerospace Medical Association Commercial Space Flight Working Group paper, *Suborbital Commercial Space Flight Crewmember Medical Issues*, Rev 11

70: Quinn C A, Lupa H & Stevenson A, *Centrifuge Training as Key Safety Mitigation in the Commercial Spaceflight Industry*, in of the 3rd IAASS Conference 'Building a Safer Space Together', 21-23 October 2008

71: Federal Aviation Administration (FAA-AST) CFR Title 14 Part 460, *Human Spaceflight Requirements*, original Docket dated 15 Dec 2006

72: International Civil Aviation Organisation (ICAO), Commercial Aviation Safety Team, *Aviation Occurrence Category Definitions and Usage Notes*, June 2004

73: Ministère de l'Equipment, des Transports et du Tourisme. Projet de loi 235uides235e à la sécurité des transports publics 235uides. PD/CM (STPG1). Paris: 1994

74: CENELEC Standard EN 50129: Railway Applications—Communications, signalling and processing systems—Safety related electronic systems for signalling. Issue: May 2002

75: SAE International, Aerospace Recommended Practice, *Safety Assessment of Transport Airplanes in Commercial Service*, ARP 5150, 2003

76: Marciacq J-B ., Morier Y., Tomasello F., Erdelyi Zs., Gerhard M., *Accommodating Suborbital flights into the EASA regulatory system*, in Proceedings of the 3rd IAASS Conference 'Building a Safer Space Together', 21-23 October 2008

77: International Space University, *Great Expectations – An Assessment of the Potential for Suborbital Transportation*, Masters Report 2008

78: Trujillo M, Sgobba T; *ESA Human Rating Requirements*, in the proceedings of the 2nd IAA Conference, Arcachon, France, 30 May – 1 June 2011

79: European Co-operation for Space Standardization, Space Product Assurance (Safety), ECSS-Q-ST-40C, 6 March 2009

80: European Co-operation for Space Standardization, Space Product Assurance (Software Product Assurance), ECSS-Q-ST-80C, 6 March 2009

81: Aerospace Corporation, George Washington University and the Massachusetts Institute of Technology; *Analysis of Human Space Flight Safety – Report to Congress*, 11 November 2008

82: European Aviation Safety Agency, *Certification Specifications for Normal, Utility, Aerobatic and Commuter Aeroplanes*, CS-23, Book 1, Airworthiness Code, 14/11/2003

83: URL; UK Health and Safety Executive, *ALARP at a glance*, http://www.hse.gov.uk/risk/theory/alarpglance.htm

84: America National Standards Institute (ANSI) GEIA STD 0010-2009, Standard Best Practices for System Safety Program Development and Execution, October 2008

85: SAE, Aerospace Recommended Practices (ARP) 4761, Guidelines and Methods for conducting Safety Assessment Process on Civil Airborne Systems and Equipment, December 1996

86: European Aviation Safety Agency, *Certification Specifications for Large Aeroplanes*, CS-25, Book 2, Acceptable Means of Compliance, 27 December 2007

87: Federal Aviation Administration (FAA). Advisory Circular AC 23-1309-1C, *Equipment, Systems and Installations in Part 23 aircraft*, dated 3 Dec 1999

88: Federal Aviation Administration (FAA-AST), Advisory Circular 431.35-1, *Expected Casualty Calculations for Commercial Space Launch and Re-entry*, dated 8/30/2000

89: International Association for the Advancement of Space Safety, Independent Space Safety Board, *Space Safety Standard for Commercial Human-Rated Systems*, March 2010

90: J Penny et.al, The Practicalities of Goal-based Safety Regulation

91: Bureau d'Enquêtes et d'Analyses. Interim Report No.2 on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro – Paris, 30 November 2009

92: Bureau d'Enquêtes et d'Analyses. Interim Report No.3 on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro – Paris, 30 November 2009

93: Federal Aviation Administration (FAA-AST), Final Environmental Assessment for the Blue Origin West Texas Commercial Launch Site, August 2006

94: Federal Aviation Administration (FAA-AST), Draft Environmental Assessment for the Oklahoma Spaceport, January 2006

95: Federal Aviation Administration (FAA-AST), Guidelines For Compliance With The National Environmental Policy Act And Related Environmental Review Statutes For The Licensing Of Commercial Launches And Launch Sites, 22 February 2001

96: Federal Aviation Administration (FAA-AST) Code of Federal Regulations Title 14 Part 420, License to Operate a Launch Site

97: Federal Aviation Administration (FAA-AST) Code of Federal Regulations Title 14 Part 437, Launch Safety, 4 Aug 2011

98: Daniel P Murray and Robert E Ellis, Air Traffic Considerations for Future Spaceports, Paper presented to the 2nd IAASS

99: Federal Aviation Administration CFR Title 14 Part 139, Certification of Airports

100: Prof. Bor R – Anxiety at 35,000ft, *An Introduction to Clinical Aerospace Psychology*, 2004, Karnak Books Ltd

101: URL: http://www.orbitaloutfitters.com/SpaceSuits.html

102: UK CAA, CAP 780, Aviation Safety Review, 2008ns

103: European Aviation Safety Agency, Certification Specification for Hot Air Balloons, CS-31HB, 2009

104: UK CAA, CAP494, British Civil Airworthiness Requirements, Part 31 – Manned Free Balloons, 2003

105: National Aeronautics And Space Administration, An Overview of the Guided Parafoil System Derived from the X-38 Experience, Jenny M. stein, Chris M. ads en^ and Alan L. Strahans

106: National Aeronautics And Space Administration, GENESIS Mishap Investigation Board Report, Volume 1, 30 Nov 2005

APPENDIX 1 - PhD Proposal – 2006

DESCRIPTION AND OBJECTIVES

Background

Travelling at 3 times the speed of sound during the ascent and experiencing 5 times Earth's nominal gravitational forces during re-entry is not a normal flight profile. Two dates will remain key moments in the new and exciting field of Space Tourism – 29th September and 4th October 2004, when Spaceship One (SS1) achieved heights of 103km and a record breaking 112km respectively. The flight was a 2-stage launch profile: the first stage was up to 50,000ft with the SS1 attached to a 'Mother-Ship' (the White Knight) to save on fuel; the second stage was the release of SS1 at 50,000ft, followed by rocket ignition taking SS1 to the pre-requisite 'space height' of 100km at 3 times the speed of sound. The spacecraft spent 5 minutes in the space environment under its own momentum and then returned through the atmosphere under gravity using a unique wing feathering system before returning to normal configuration and gliding back to the departure runway.

How does the general public, let alone highly trained flight crew, cope with these and other exacting environmental factors during a suborbital spaceflight? To enable the innovative space tourism industry to achieve success, designers and operators must constantly view the challenge from a safety perspective. The Federal Aviation Administration (FAA) has produced regulatory guidelines to cover the varying design proposals of prospective Re-Launch Vehicle (RLV) operators and these guidelines provide baseline measures. The challenge for the RLV Operators is to employ safety criteria to meet and exceed the guidelines.

Project Description

The aim of this project is to examine how, and if, introducing a safety management system from scratch can influence the commercial space travel industry. In particular, I will be introducing a holistic Safety Management System (SMS) and will review different approaches. Due to the complexities of space travel, I review the Safety Case approach, including the Goal Structured Notation (GSN) methodology. During the implementation of the SMS, I will be able to examine the influence from a 'Through Life Management Plan' (TLMP) perspective, including environmental legislative requirements. Spaceports and Spaceflight Training will also be discussed as part of Industry's business and safety integration.

New and Raw Data

I aim to produce a survey questionnaire on Safety and should have access to the prospective Space Tourists. I aim to analyse the results and correlate these to the proposed mitigation measures and discuss any gapped issues.

Having access to Medical data during the pre-flight screening and training will give another input to the SMS and mitigation factors to consider.

I would then aim to instigate a Test Phase questionnaire for pilots and other flight crew and analyse the results, once again looking at further mitigation factors, as appropriate. Also, during this phase, I would integrate my investigations with the Medical telemetry, looking at whether mitigating measures were effective, or whether further measures are required in design, procedures or training.

Finally, during the first few months of the In-Service Phase, useful data from passenger surveys and medical telemetry would give valuable knowledge from which to instigate change management, as appropriate.

The holistic programme should evolve along the following path:

Design Phase

It is essential to have senior management 'buy-in' to safety management at the beginning and to resource this accordingly; Safety Policy statement from the company President/CEO is the start.
It is critical to begin constructing the safety case framework and the Hazard Log. From this, I would expect to demonstrate the influence of the SMS (safety by design) in mitigating hazards by:

- modification to the design
- introduction of operational procedures
- training

Test Phase

- Examining the difference of 'As Designed' and 'As Flown' safety cases.
- Change Management; adjustments to design, procedures and training may be required and an effective SMS, incorporating documented change management procedures.
- Psychological and Physiological aspects to be managed from the crew's perspective and then adapted for the general public.
- Pre-Operations phase passenger survey on safety perspectives.
- Assessment of training and medical telemetry results of crew and test subjects.

In-Service Phase

- Monitoring of initial space flights and examining results/surveys from the general public – to include medical telemetry of passengers.
- Change & Risk Management strategies.

Objectives

- Primary. My primary objective is to provide an effective SMS solution to commercial spaceflight operations and activities, whilst examining the influences of safety management during the project.
- Secondary. My secondary objectives are to provide an assessment of the next steps to orbital operations, with respect to differences in psychological and physiological requirements.

RESOURCES

I intend to use the following sources:
Correspondence and meetings with different RLV Operators
Visits/ Seminars/ Courses/ Surveys/ Related books, magazine articles/ Internet sites
Primary experience in introducing an SMS
Primary experience on the proposed training schedule
Having read a previous students PhD dissertation

OUTLINE OF MAIN CHAPTERS

Introduction
Review of Space Tourism Regulations
Review of SMS
Review of Hazard and Risk Management
Review of Safety Case methodology
Examine Influence of SMS during design, test and In-Service phases
Examine different RLV Operator's approach to safety
Examine the role of Safety & Environmental Management at Spaceports
Examine the role of Spaceflight Training for Flight Crew & Passengers
A look at future Orbital Space Travel challenges
Recommendations
Summary, Conclusions, Further Work

TIMESCALE

Apr/May 06	-	PhD approval
2006-9	-	Examination of SMS influence
2008/9	-	Write-up first draft
2009	-	Revise/re-write as appropriate to final draft

APPENDIX 2 – Timeline of Related Research Activities

Activity Date	Spaceflight/Research Activity	General Topic	Specific Presentation/ Meeting	Remarks
Sep 2006	**Introductory Meeting** with City University to kick-off suborbital space research	Kick-Off meeting to discuss research possibilities	Meeting	
Sep 2006	**Conference** – 56th IAC Valencia	Space Conference	Paper & Presentation on SMS for commercial spaceflight	First presentation at major event – well received and interesting discussions on topic with Director of BNSC
May 2007	**Conference** - 2nd IAASS, Chicago	Space Safety conference	Networking Information gathering	Varying lectures from NASA/ESA and more specifically from the FAA on Commercial Spaceflight
June 2007	**Microgravity paper** presented to QinetiQ for discussions with UK CAA	Possibility of certification of microgravity flights in the UK	Paper	Meeting with the UK CAA was positive in that they would be receptive to submission of microgravity aircraft (modified)
May 2008	**Conference** – 1st IAA, Arcachon, France	Space Conference	Meeting with Rocketplane VP (Chuck Lauer)	Reasonable conference no progress in regulations for personal spaceflight. Meeting with Chuck Lauer very positive Jan 2008
Sep 2008	**Space Tourism Presentation** to Kingswood School, Bath	Spaceflight Presentation	Presentation	First presentation on generic personal spaceflight
Oct 2008	**Conference** – 3rd IAASS, Rome	Space Safety conference	Paper & Presentation on Centrifuge as key mitigation for personal spaceflight. Networking. Information gathering.	Excellent conference with more focus on emerging commercial field – good contacts with EASA/ESA reps and follow-up phone interview by Rob Coppinger (Flight International/Global)
Oct 2008	University of Bath – **External Supervisor**	External supervisor appointed – Professor Paul Maropoulous, Head of Mech. Eng. at University of Bath	Kick-off meeting	Discussion on status and way forward
Jan 2009	**Space Tourism Presentation** to the MKAS, Milton Keynes	Spaceflight Presentation	Presentation	Updated presentation on generic personal spaceflight
Feb 2009	**Space Tourism Presentation** to the IET, University of Bath	Spaceflight Presentation	Presentation	Updated presentation on generic personal spaceflight
May 2009	City University – **Update on PhD**	Update to course director on PhD status and way forward	Presentation/meeting	
May 2009	University of Bath – External Supervisor review	Review of strategy change to dissertation	Meeting	
June 2009	**Conference** – RAeS Space Tourism, London	Space Conference	Exhibition stand for Worldview Spaceflight with Rocketplane material, model (partnership formed)	Investor now on board and able to start effective marketing strategy to raise profile of personal spaceflight training – benefit to

Activity Date	Spaceflight/Research Activity	General Topic	Specific Presentation/ Meeting	Remarks
				research will be from training analysis and raw data and surveys
Dec 2009	University of Bath – External Supervisor review	Review of progress	Meeting	
May 2010	**Conference** – 4th IAASS, Huntsville	Space Safety conference	Paper & Presentation on Safety Criteria for personal spaceflight. Also sat on suborbital space safety panel discussion.	The panel discussion was a great opportunity to raise my profile and to get my points across in a wide forum
Nov 2010	**Conference** – Inside Government: Space, London	Space Conference	Networking Information gathering	Varying lectures from UK Space Agency; more specifically concerning satellites but did go into emerging space tourism
Dec 2010	City University – Update on PhD	Update to course director on PhD status and way forward	Presentation/meeting	
Dec 2010	University of Bath – External Supervisor review	Review of progress	Meeting	
Feb 2011	**EASA Meeting**, Cologne, Germany	Meeting to go through the Pre-Regulatory Impact Assessment that I contributed to and discuss the next steps for the full SoA Policy and AMC/GM	Per previous column	Excellent first meeting and detailed next steps and next meeting
April 2011	City University – Update on PhD	Update to course director on PhD status and way forward	Presentation/meeting	
May-June 2011	**Conference** – 2nd IAA Access to Space	2ND conference to update progress in the private space industry	Attendance for information gathering and networking	Good conference but showed that progress was slow in the private spaceflight domain (suborbital)
August 2011	City University – Draft PhD Complete	Update to course director on PhD status and way forward	Presentation/meeting	
Oct 2011	Conference – 5th IAASS, Paris	Space Safety conference	Paper & Presentation on Safety Model for personal spaceflight. Also sat on suborbital space safety panel discussion. Also now Chair of Suborbital Technical Committee – also organised a suborbital workshop session	The panel discussion is a great opportunity to raise my profile and to get the main points across in a wide forum
Dec 2011	VIVA	Present Thesis		
2012	Graduation			

APPENDIX 3 – Case Study for '*SATURN SAFETY MODEL'* (Air France Flight 447 Disaster)

SYNOPSIS [91]:

Date of accident	1st June 2009 at around 2 h 15 (UTC)	
Site of accident	Near the TASIL point, in international waters, Atlantic Ocean	
Type of flight	International public transport of passengers Scheduled flight AF447	
Aircraft	Airbus A330-203 registered F-GZCP	(Aircraft Destroyed)
Owner	Air France	
Operator	Air France	
Persons on board	Flight crew: 3 Cabin crew: 9 Passengers: 216	(All on board killed)

Summary

On 31 May 2009, flight AF447 took off from Rio de Janeiro Galeão airport bound for Paris Charles de Gaulle. The airplane was in contact with the Brazilian ATLANTICO ATC centre on the INTOL – SALPU – ORARO route at FL350. There were no further communications with the crew after passing the INTOL point. At 2 h 10, a position message and some maintenance messages were transmitted by the ACARS automatic system.

At around 2 h 02, the Captain left the cockpit. At around 2 h 08, the crew made a course change of about ten degrees to the left, probably to avoid echoes detected by the weather radar.

At 2 h 10 min 05, likely following the obstruction of the Pitot probes in an ice crystal environment, the speed indications became erroneous and the automatic systems disconnected. The airplane's flight path was not brought under control by the two co-pilots, who were re-joined shortly after by the Captain. The airplane went into a stall that lasted until the impact with the sea at 2 h 14 min 28.

Bodies and airplane parts were found from 6 June 2009 onwards by the French and Brazilian navies.

Notable Issues

The cases of inconsistencies in measured speeds are classified as *major* in the safety analysis that describes the associated failure conditions.

Airbus presented 17 cases of temporary Pitot blocking that had occurred on the long-range fleet between 2003 and 2008, including 9 in 2008 without being able to explain this sudden increase.

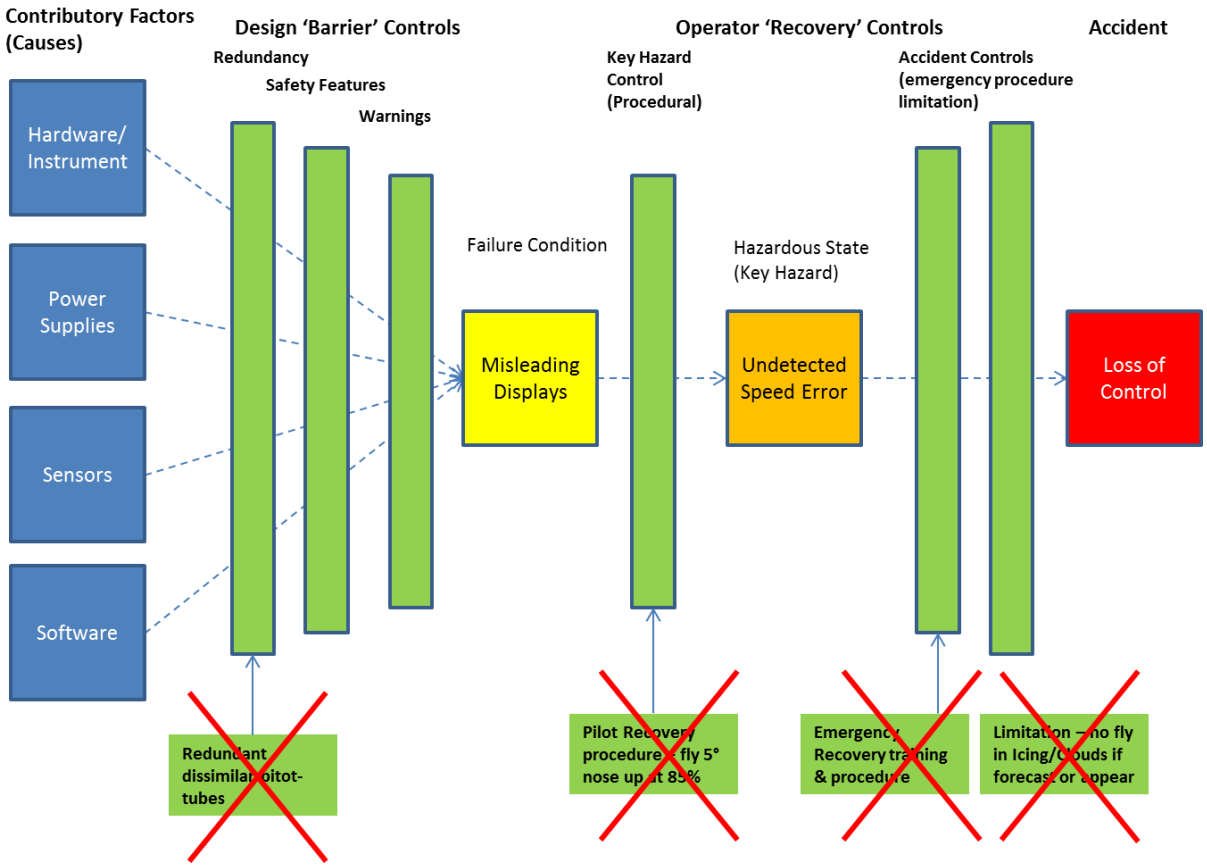
The first batch of C16195BA Pitot probes arrived at Air France on 26 May 2009, that is to say six days before the F-GZCP accident (existing probes were C16195AA type).

SATURN SAFETY MODEL ANALYSIS:

By using the *SATURN SAFETY MODEL* we can examine the sequential components and determine those that failed. In the figure below we can see that the following controls failed:

- Redundant sensors – the 3 pitot tubes were the same and therefore were subject to common mode failures

- Key (Platform) Hazard procedural control failure – operating procedure to control the aircraft for '*Unreliable Indicated Airspeed* (IAS)' (at 5 degrees nose up and 85 per cent power is the standard procedure);
  [Although having identified and called out the loss of the speed indications, neither of the two co-pilots called the procedure "Unreliable IAS"] [92]
- Emergency recovery procedures (and training) – once passed the hazardous state of undetected speed error the pilot should have recovered the aircraft before the onset of stall i.e. the warnings of stall normally include 'stick-shakers' and warning horns; *neither of the pilots formally identified the stall situation* [92]. Had they done so (and had the appropriate training) they would have pushed the nose of the aircraft down to regain airspeed and hence lift over the wings. The author (previously a Flight [Air] Engineer) has practised stall procedures as part of flight crew drills both in normal training and in recurrent simulator training on the VC10 aircraft. Additionally crews were trained on 'wind-shear' approaches and this involved 'riding' the stall warning systems with full power. This sort of training was not conducted by the two co-pilots according to the BEA report [93].
- No Limitations in place either to;
  - Avoid the altitude that the pitot-tubes could be subject to super-cooled water droplets and icing i.e. fly below Flight Level 310 (this would require more fuel to be carried to cross the Atlantic)
  - Avoid Flight in Icing conditions and flight in or near thunderstorms i.e. fly around (divert off track) any Cumulonimbus clouds (this would require more fuel to be carried if the forecast indicated clouds)



FINAL REPORT ON THE ACCIDENT:

The BEA Interim Report No.3 states that Air France has introduced the operator control measures in terms of briefing, training (in simulators) and revised the *Unreliable IAS* procedures. Also the design measures required of the SB have been implemented and so the Safety Risk is now down to a Tolerable level of risk

APPENDIX 4 – Case Study for '*SATURN SAFETY MODEL'* (Space Shuttle Challenger & Columbia Disasters)

SYNOPSIS:

Date of accidents	28 Jan 1986 – Challenger 01 Feb 2003 – Columbia	
Site of accidents	Challenger – Launch Columbia – Re-entry	
Type of flights	International Space Station standard NASA spaceflights	
Vehicles	Challenger – Space Shuttle Columbia – Space Shuttle	(Challenger Exploded) (Columbia broke up - structural failure)
Owner/Operator	NASA	
Persons on board	Challenger Astronauts: 7 Challenger Astronauts: 7	(All on board killed) (All on board killed)

SUMMARIES:

Challenger – On 28 Jan 1986 Space Shuttle Challenger launched at 0500hrs (US time) after having been delayed from previous launches. Seconds after Launch Challenger's Expendable Rocket Boosters exploded, destroying the Space Shuttle System; all on board were killed in the 'mishap'.

Columbia – On 01 Feb 2003 Space Shuttle Columbia was re-entering Earth's atmosphere. On its Launch from Earth, a protective thermal foam tile was seen to be dislodged and then striking the leading edge of the main-plane. Whilst in Space the area was examined but NASA considered that a repair could not be undertaken and so authorised the return. Columbia suffered structural failure of the main-plane during re-entry due to the excessive heat and broke up; all on board were killed in the 'mishap'.

Notable Issues:

NASA safety culture was cited as 'lamentable' by Diane Vaughan and this was further backed up by Rd. Richard Freeman despite the 17 year gap between the accidents.

Challenger: The management played a large part in the Challenger disaster in that they authorised a Launch when the temperatures were extremely low and this was against the advice of the engineers who knew that the O-Ring seals had a history of blow-backs at low temperatures.

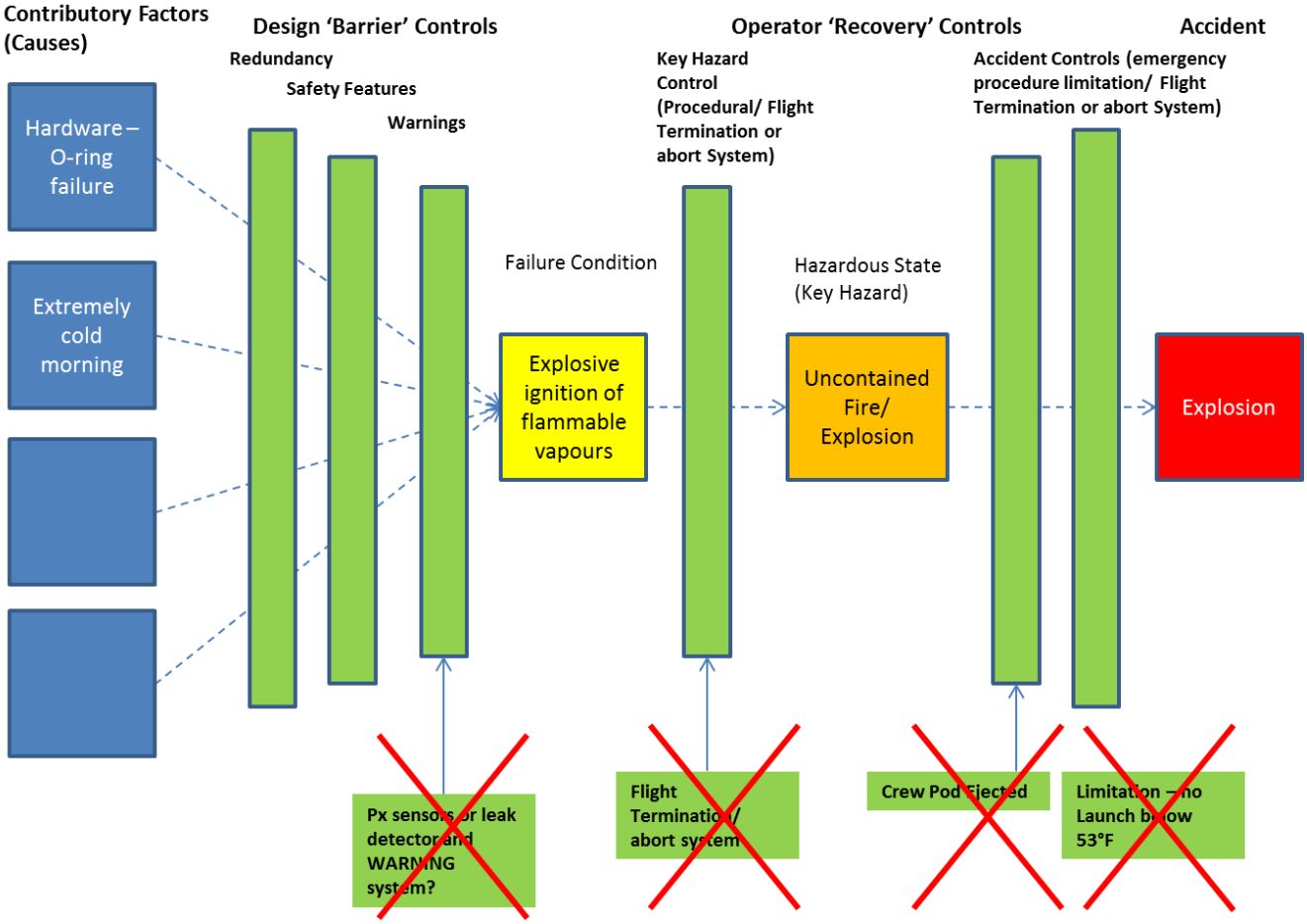
Columbia: The management also played a large part in the Columbia disaster as the displacement of foam tiles was known to be an issue and the video evidence clearly showed a tile striking the leading edge of Columbia on Launch. Although the damage was assessed whilst docked the ISS the decision to return the Space Shuttle with full crew was flawed.

SATURN SAFETY MODEL ANALYSIS:

By using the *SATURN SAFETY MODEL* we can examine the sequential components and determine those that failed. In the figure below we can see that the following controls failed firstly for Challenger and then for Columbia:

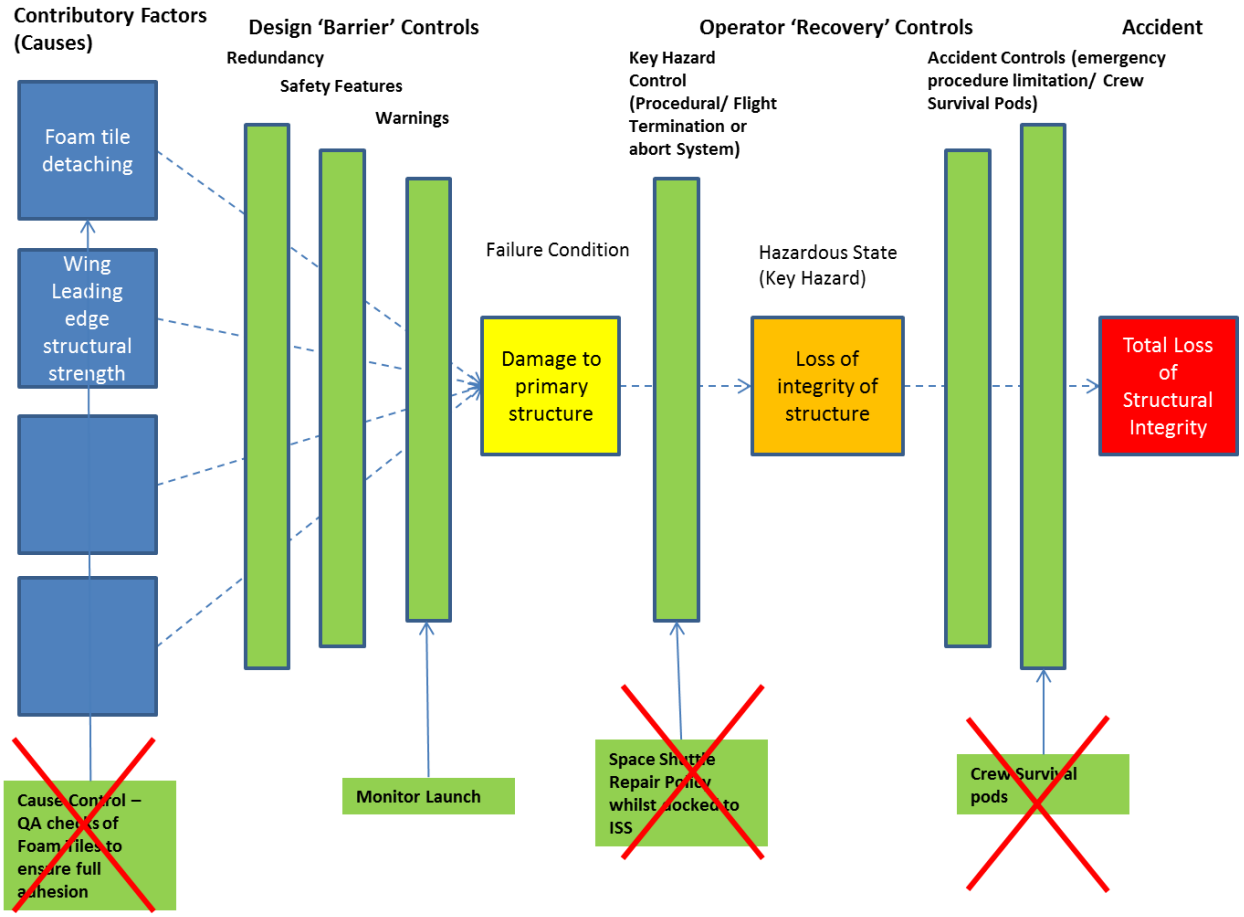
Challenger Sequence detailed below:

- Pressure sensors not providing sufficient data in time
- Flight Termination System – not able to protect the astronauts in time
- Crew Pod ejection – not able to protect the astronauts in time
- Limitation ignored – the 53° F limitation for the O-Rings were ignored by the management against the engineer's advice



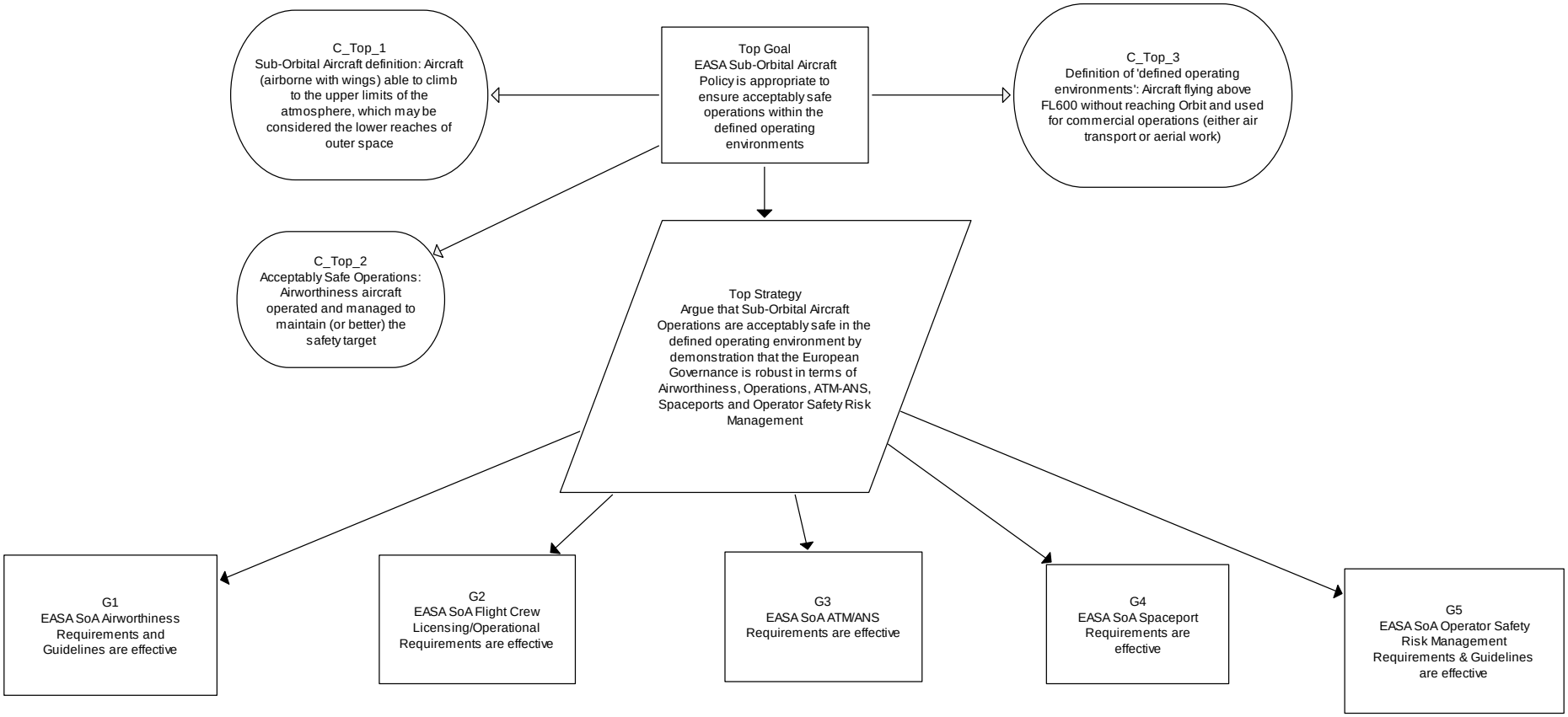
Columbia Sequence detailed below:

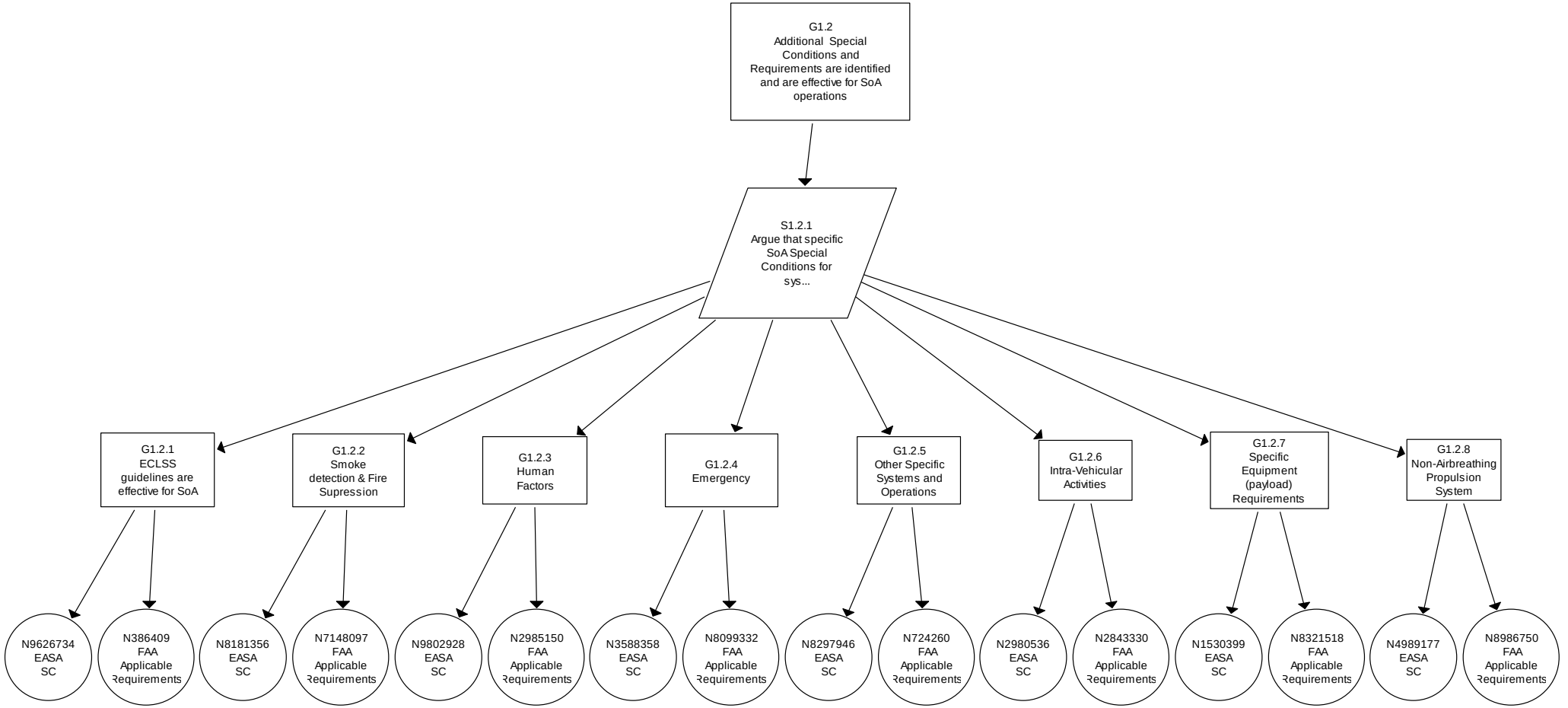
- Cause Control failure – Lack of Quality Assurance to check the adhesive properties of the heat resistant foam tiles
- Lack of Space Shuttle repair policy whilst docked at the ISS (leading to decision to return Columbia without repair)
- Crew Pod ejection – low survivability; as the airframe started to break up the crew should have been able to eject the crew pod safely and float the Earth. This facility was not properly thought out

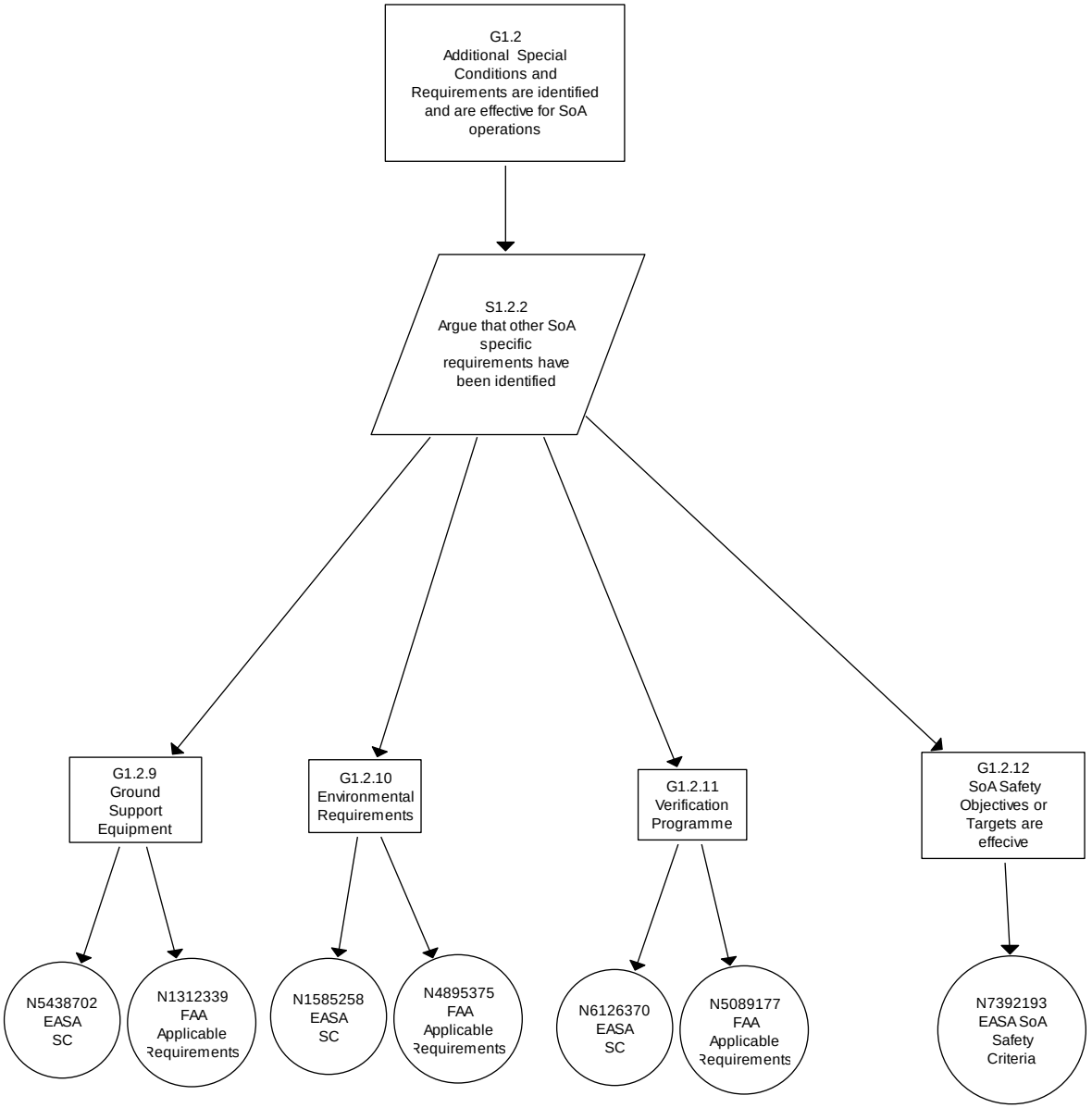

Contributory Factors (Causes)
Design 'Barrier' Controls
Redundancy
Safety Features
Warnings
Operator 'Recovery' Controls
Key Hazard Control (Procedural/ Flight Termination or abort System)
Accident
Accident Controls (emergency procedure limitation/ Crew Survival Pods)
Foam tile detaching
Wing Leading edge structural strength
Failure Condition
Damage to primary structure
Hazardous State (Key Hazard)
Loss of integrity of structure
Total Loss of Structural Integrity
Cause Control – QA checks of Foam tiles to ensure full adhesion
Monitor Launch
Space Shuttle Repair Policy whilst docked to ISS
Crew Survival pods

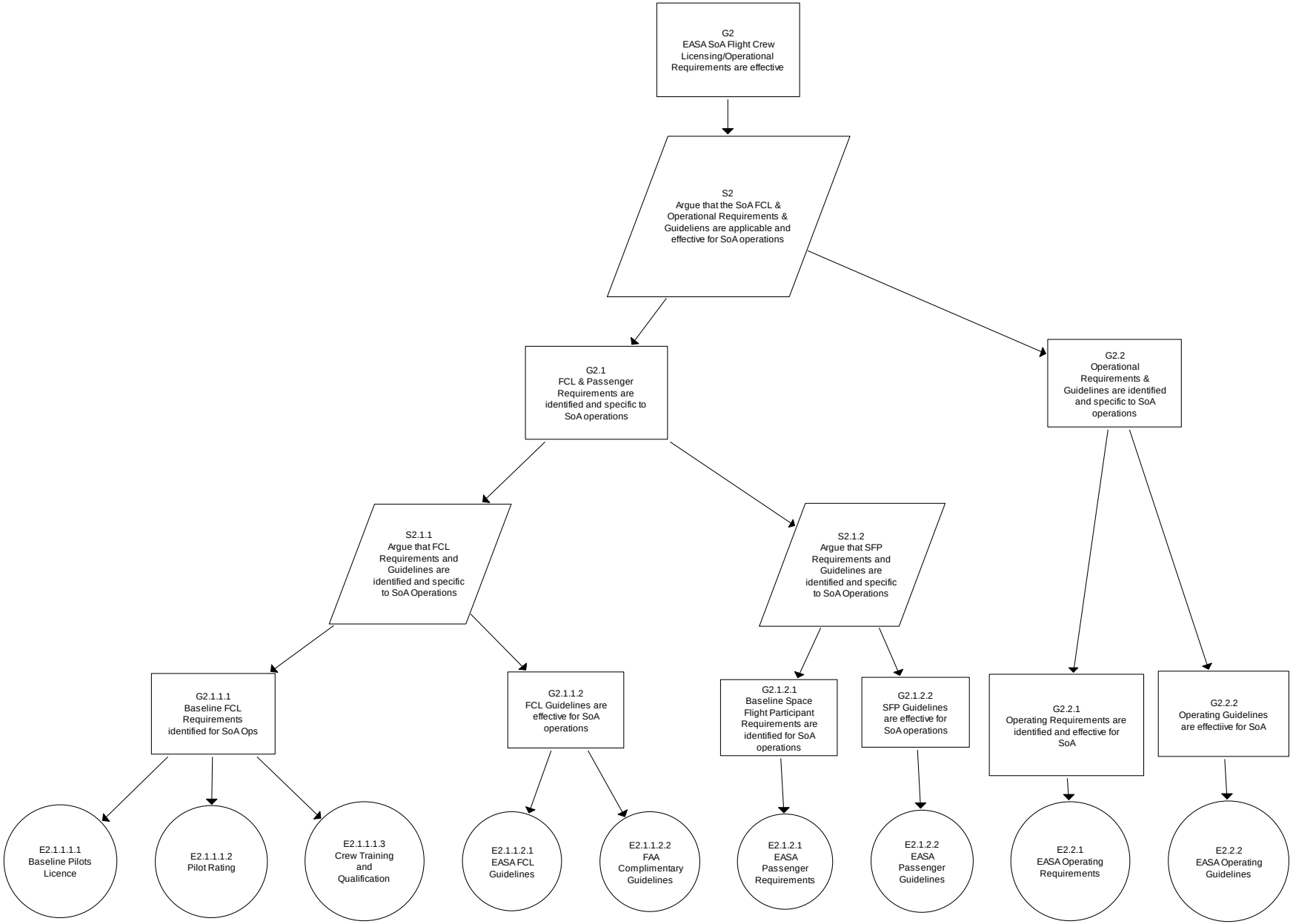
APPENDIX 5 - Suborbital Aircraft Policy – Goal Structuring Notation

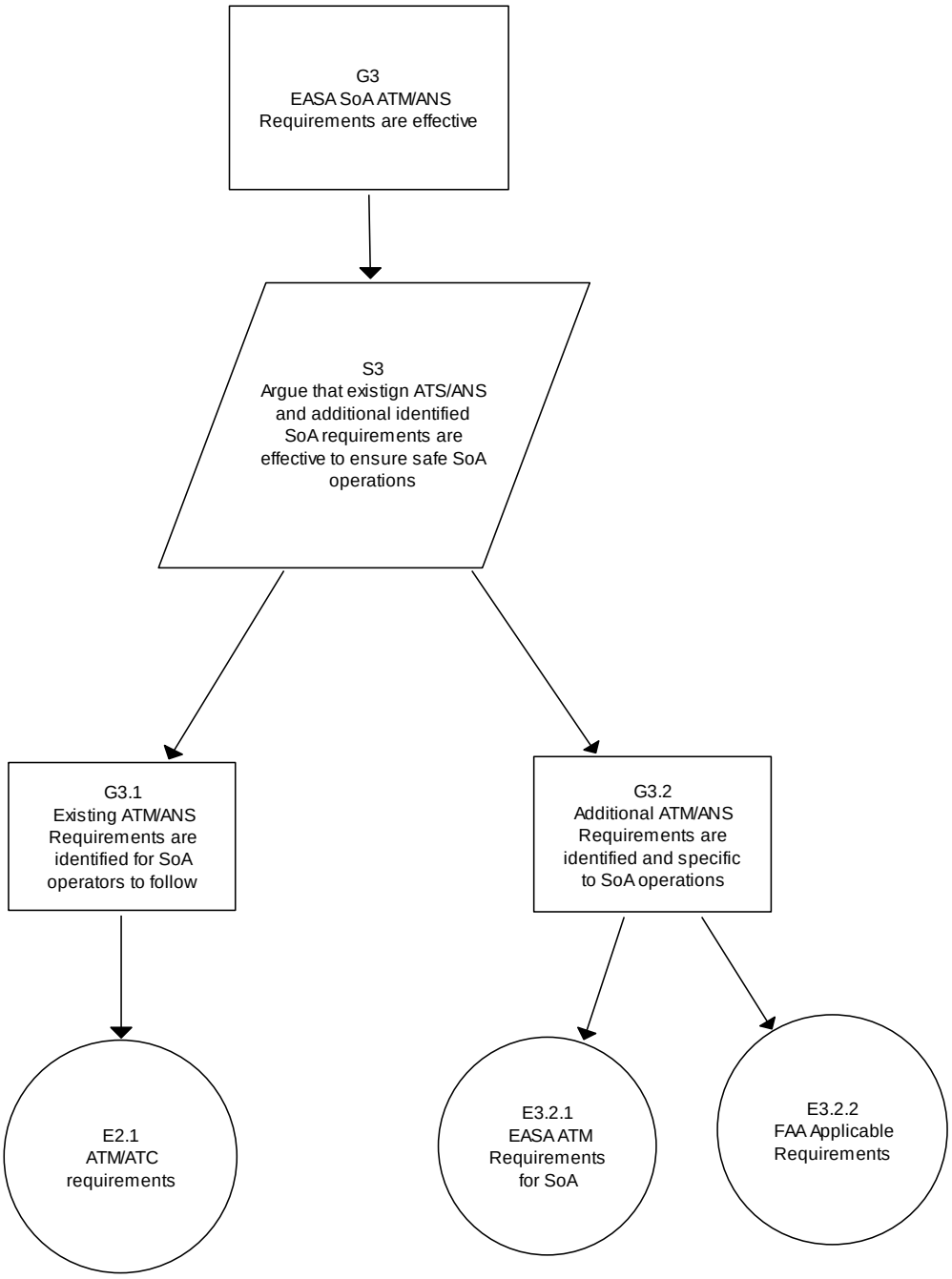
This task is not complete at the time of submission due to EASA suspending the task pending the European Commission's decision to proceed from the information provided for the Preliminary Regulatory Impact Assessment (RIA). The following Safety Argument requires substantiation and further work when EASA have the approval to continue.

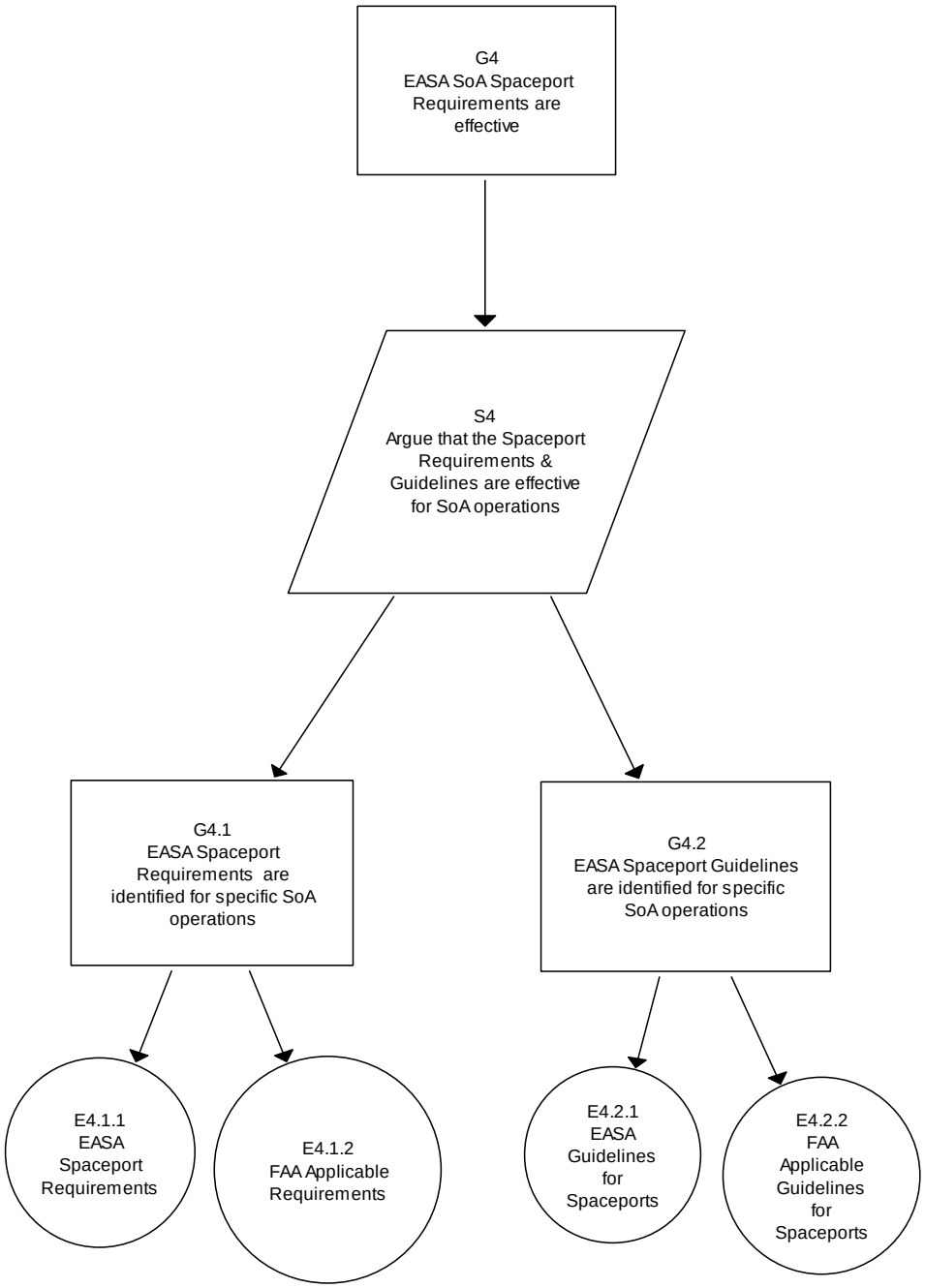


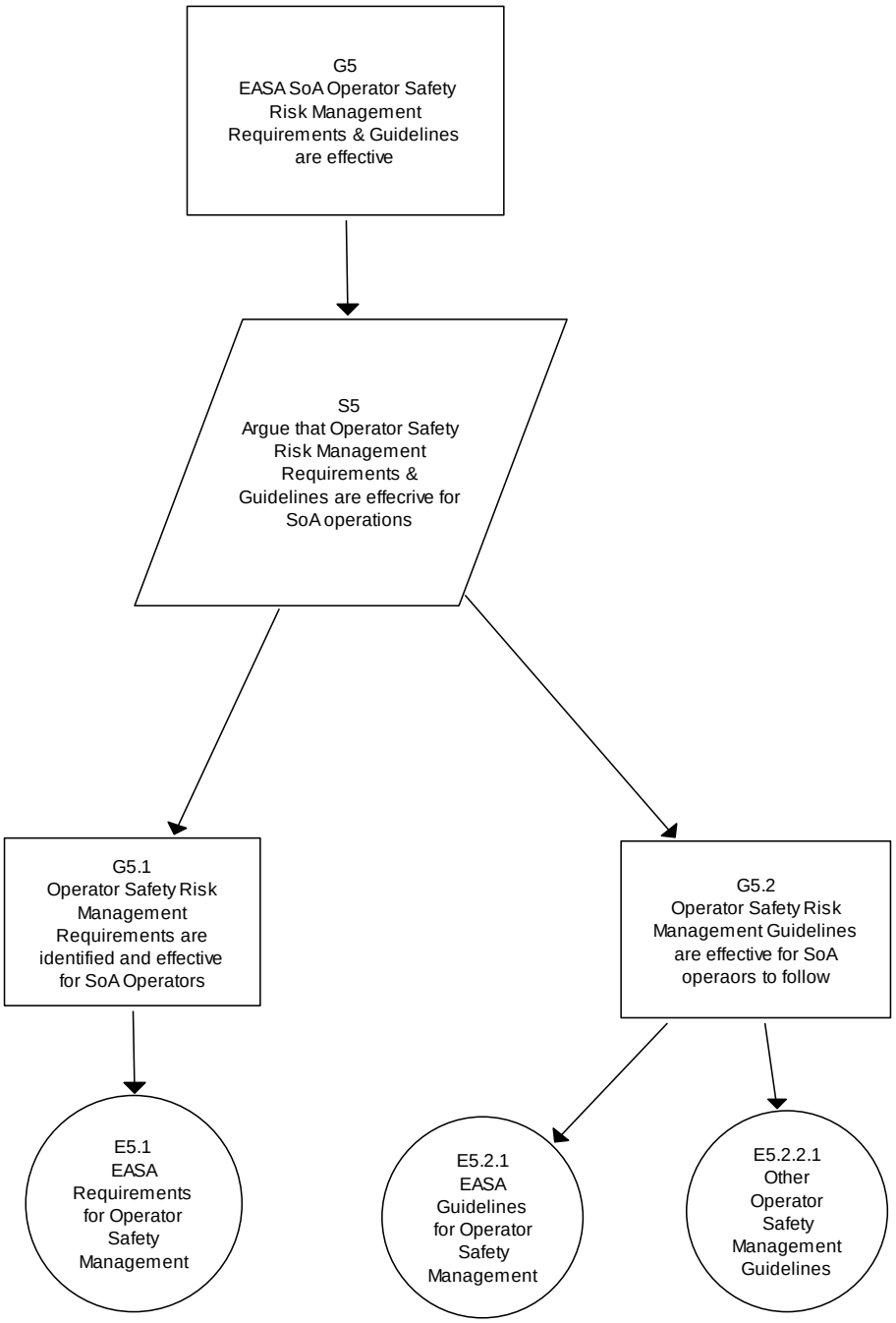

G1.2
Additional Special Conditions and Requirements are identified and are effective for SoA operations
S1.2.1
Argue that specific SoA Special Conditions for sys...
G1.2.1
ECLSS guidelines are effective for SoA
G1.2.2
Smoke detection & Fire Supression
G1.2.3
Human Factors
G1.2.4
Emergency
G1.2.5
Other Specific Systems and Operations
G1.2.6
Intra-Vehicular Activities
G1.2.7
Specific Equipment (payload) Requirements
G1.2.8
Non-Airbreathing Propulsion System
N9626734
EASA SC
N386409
FAA Applicable Requirements
N8181356
EASA SC
N7148097
FAA Applicable Requirements
N9802928
EASA SC
N2985150
FAA Applicable Requirements
N3588358
EASA SC
N8099332
FAA Applicable Requirements
N8297946
EASA SC
N724260
FAA Applicable Requirements
N2980536
EASA SC
N2843330
FAA Applicable Requirements
N1530399
EASA SC
N8321518
FAA Applicable Requirements
N4989177
EASA SC
N8986750
FAA Applicable Requirements


G1.2
Additional Special Conditions and Requirements are identified and are effective for SoA operations
S1.2.2
Argue that other SoA specific requirements have been identified
G1.2.9
Ground Support Equipment
G1.2.10
Environmental Requirements
G1.2.11
Verification Programme
G1.2.12
SoA Safety Objectives or Targets are effecive
N5438702
EASA
SC
N1312339
FAA
Applicable
Requirements
N1585258
EASA
SC
N4895375
FAA
Applicable
Requirements
N6126370
EASA
SC
N5089177
FAA
Applicable
Requirements
N7392193
EASA SoA
Safety
Criteria


G2
EASA SoA Flight Crew Licensing/Operational Requirements are effective
S2
Argue that the SoA FCL & Operational Requirements & Guideliens are applicable and effective for SoA operations
G2.1
FCL & Passenger Requirements are identified and specific to SoA operations
G2.2
Operational Requirements & Guidelines are identified and specific to SoA operations
S2.1.1
Argue that FCL Requirements and Guidelines are identified and specific to SoA Operations
S2.1.2
Argue that SFP Requirements and Guidelines are identified and specific to SoA Operations
G2.1.1.1
Baseline FCL Requirements identified for SoA Ops
G2.1.1.2
FCL Guidelines are effective for SoA operations
G2.1.2.1
Baseline Space Flight Participant Requirements are identified for SoA operations
G2.1.2.2
SFP Guidelines are effective for SoA operations
G2.2.1
Operating Requirements are identified and effective for SoA
G2.2.2
Operating Guidelines are effectiive for SoA
E2.1.1.1.1
Baseline Pilots Licence
E2.1.1.1.2
Pilot Rating
E2.1.1.1.3
Crew Training and Qualification
E2.1.1.2.1
EASA FCL Guidelines
E2.1.1.2.2
FAA Complimentary Guidelines
E2.1.2.1
EASA Passenger Requirements
E2.1.2.2
EASA Passenger Guidelines
E2.2.1
EASA Operating Requirements
E2.2.2
EASA Operating Guidelines


G3
EASA SoA ATM/ANS
Requirements are effective
S3
Argue that existign ATS/ANS
and additional identified
SoA requirements are
effective to ensure safe SoA
operations
G3.1
Existing ATM/ANS
Requirements are
identified for SoA
operators to follow
G3.2
Additional ATM/ANS
Requirements are
identified and specific
to SoA operations
E2.1
ATM/ATC
requirements
E3.2.1
EASA ATM
Requirements
for SoA
E3.2.2
FAA Applicable
Requirements


G4
EASA SoA Spaceport Requirements are effective
S4
Argue that the Spaceport Requirements & Guidelines are effective for SoA operations
G4.1
EASA Spaceport Requirements are identified for specific SoA operations
G4.2
EASA Spaceport Guidelines are identified for specific SoA operations
E4.1.1
EASA Spaceport Requirements
E4.1.2
FAA Applicable Requirements
E4.2.1
EASA Guidelines for Spaceports
E4.2.2
FAA Applicable Guidelines for Spaceports


G5
EASA SoA Operator Safety Risk Management Requirements & Guidelines are effective
S5
Argue that Operator Safety Risk Management Requirements & Guidelines are effecrive for SoA operations
G5.1
Operator Safety Risk Management Requirements are identified and effective for SoA Operators
G5.2
Operator Safety Risk Management Guidelines are effective for SoA operaors to follow
E5.1
EASA Requirements for Operator Safety Management
E5.2.1
EASA Guidelines for Operator Safety Management
E5.2.2.1
Other Operator Safety Management Guidelines

EASA Suborbital Aircraft Policy Task

This task is not complete at the time of submission due to EASA suspending the task pending the European Commission's decision to proceed from the information provided for the Preliminary Regulatory Impact Assessment (RIA).

Task Outline: The task was to assist EASA in developing a Policy and Guidance Material for Suborbital Aircraft (SoA) operations. This was to be achieved partially by the Gap Analysis of the FAA-AST Regulations and Guidelines and to determine which existing EASA Regulations and Guidance would be applicable to SoA operations.

Task Structure: The SoA Policy is in essence a set of requirements and guidance material that prospective designers and operators will follow in order to certify their vehicle within the existing EASA regulatory framework with Special Conditions levied as appropriate. Therefore this is a goal-based regulatory approach and the author has provided a safety argument structured to suit a goal-based approach.

Task Status: The argument presented by the Goal Structuring Notation (GSN) in the figures above represent the SoA Policy. The report generated from the GSN (using the ASCE Tool) is presented below. The status is that the arguments and evidence are not fully substantiated at the time of submission. This is made clear within the main body of the thesis and a recommendation made to continue with the task as further work when the EC approves the task for EASA to continue.

Within the report below those aspects that are not complete are essentially those that have a simple statement or placeholder with no further argument or no further evidence provided i.e. 'Smoke Detection & Fire Suppression'; here it is the intent that the EASA requirements will be stated (these may be existing standard Certification Specification Requirements) and also any relevant FAA-AST requirements will be stated (some of these are not relevant for certification considerations and are not included whereas others are relevant or indeed relevant but with caveats).

EASA Suborbital Aircraft Policy

Top Goal

EASA Suborbital Aircraft Policy is appropriate to ensure safe operations within the defined operating environments

Context 1

Suborbital Aircraft definition: Aircraft (airborne with wings) able to climb to the upper limits of the atmosphere, which may be considered the lower reaches of outer space

Context 3

Definition of 'defined operating environments': Aircraft flying above FL600 without reaching Orbit and used for commercial operations (either air transport or aerial work)

Context 2

Acceptably Safe Operations: Airworthiness aircraft operated and managed to maintain (or better) the safety target

Top Strategy

Argue that Suborbital Aircraft Operations are acceptably safe in the defined operating environment by demonstration that the European Governance is robust in terms of Airworthiness, Operations, ATM-ANS, Spaceports and Operator Safety Risk Management

Justification to Strategy

The argument will be justified by the public workshop and invited comments to the NPA; therefore the final Policy will be ratified by EASA and the Industry

Goal 1 - EASA SoA Airworthiness Requirements and Guidelines are effective

Argument 1.1

Argue that EASA Airworthiness Requirements and Guidelines are robust for SoA operations

Goal 1.1 - Applicable Basic Requirements are effective for SoA operations

Evidence 1.1.1

EASA Regulations EC No. 216/2008

E1.1.2

Regulations (EC) No. 1702/2003 (Part 21)

E1.1.3

EASA Certification Specifications (CS-23)

Goal 1.2 - Additional Requirements are identified and are effective for SoA operations

Argument 1.2

Additional Requirements are identified and are effective for SoA operations

Goal 1.2.1

ECLSS guidelines are effective for SoA

Goal 1.2.2

Smoke detection & Fire Suppression

Goal 1.2.3

Human Factors

G1.2.4

Emergency

G1.2.5

Other Specific Systems and Operations

G1.2.6

Intra-Vehicular Activities

G1.2.7

Specific Equipment (payload) Requirements

G1.2.8

Non-Air breathing Propulsion System

G1.2.9

Ground Support Equipment

Argue that other SoA specific requirements have been identified

G1.2.10

Environmental Requirements

G1.2.11

Verification Programme

G2 - EASA SoA Flight Crew Licensing/Operational Requirements are effective

Argument 2

Argue that the SoA FCL & Operational Requirements & Guidelines are applicable and effective for SoA operations

Goal 2.1 - FCL & Passenger Requirements and Guidelines are identified and specific to SoA operations

Substantiated by Goals G2.1.1 & G2.1.2

Strategy 2.1.1 - Argue that FCL Requirements and Guidelines are identified and specific to SoA Operations Baseline Flight Crew Qualification:

EASA considers that Flight Crew Licensing (FCL) requirements are at (as a minimum) the equivalence of that commensurate with airline pilots i.e. that an Air Transport License (ATPL) or Commercial License should be held.

Rating:

Flight Test Pilot (or military fast jet pilot) in the absence of a specific SoA rating may be considered.

Flight Crew Medical Standards:

EASA considers that Flight Crew should hold a Class I aerospace medical certificate.

Flight Crew Training:

Flight Crew Training shall be performed using representative hardware and applying standards for Training Records and CQRM [FAA-AST 460.7]

G2.1.1.1 - Baseline FCL Requirements identified for SoA Ops

Standard Pilot Requirements

Current EASA standard Airline Transport Pilot Licence (ATPL) or Commercial Pilots Licence is the minimum requirement for Flight Crew to be considered to undertake SoA flights.

Alternate Acceptable Requirements

In the absence of an ATPL or CPL, a pilot can fly SoA if a Flight Test Pilot rating is held. This includes ex-military fast jet test pilots in particular as long as this is with currency.

Additional Requirements

1. Should a pilot only hold and ATPL or CPL, they must complete an Operators training program (including centrifuge training)
2. Should a pilot not hold an ATPL or CPL, he must hold a test-pilot rating (fast jet) AND the operator must ensure that at least one pilot holds an ATPL or CPL in order to fly through the NAS.

Medical Requirements

EASA requirements are for the highest standards for flight crew due to the complex flight environment conditions. A Class I aerospace medical certificate is required.

Training Standards

FAA-AST standards for Flight Crew training are considered appropriate for EASA standards and detail the following [*FAA-AST Human Spaceflight CFR 460]:*
The operator should develop a mission- and configuration-specific training program for flight crew and define standards in accordance with paragraph c for successful completion in order to (1) cover all phases of flight using i) a method of simulation, ii) an aircraft with similar characteristics iii) incremental expansion of the mission envelope, or iv) an equivalent method of training. AND (2) the operator should verify through test, analysis, inspection or demonstration that any flight crew training device realistically represents the vehicle's configuration and mission AND (3) nominal and non-nominal flight conditions AND (4) transition between multiple control and/or propulsion modes.
Additionally, it is required that all SoA pilots undergo centrifuge training in both Gx and Gz axis in order to demonstrate compatibility and competence in dealing with high-g loads.

G2.1.1.2 - FCL Guidelines are effective for SoA operations

EASA Flight Crew Licensing Guidelines

The FAA-AST guidelines [*Human Spaceflight CFR 460*] state that '*the pilot of an RLV that will operate in the National Airspace System (NAS) should possess an FAA pilot certificate, and should hold ratings to operate one or more aircraft with similar characteristics for as many phases of the mission as practicable'*.
EASA concurs with the general statement on FCL and have further split the requirements as detailed in section G2.1.1.1. The rationale is that it is anticipated that the initial pilots will stem from the military fast-jet test pilot (and non-test pilot) community and these will be well suited to fly in the high g-force environment. It is recognised that the SoA operations will take place in the NAS and therefore at least one pilot should hold an ATPL or CPL in addition to the test pilot/fast-jet pilot rating.

Flight Crew Medical Guidelines

EASA requirements stipulate a Class I Aerospace Medical certificate, as opposed to a Class II certificate. The rationale is that a Class II may be sufficient to obtain an ATPL which is generally flown in a benign environment (emergencies excepted) and therefore due to the high g-forces and

other complex environment aspects it is considered that higher medical standards are required for SoA operations.
Additionally Flight Crew should be provided with passive radiation dosimeters so that their exposure can be monitored; it is proposed that an annual limit of 50mSv and a career limit of 100mSv is enforced by operators (it is anticipated that a typical annual dosage may be in the order of 7-15 mSv).

Flight Crew Training Standards

EASA Flight Crew Training Standard principles agree with the FAA-AST approach, in that training should be performed using representative hardware and applying standards for Training Records and CQRM [*FAA-AST 460.7*]. In addition offer the following guidelines for operators:

- Centrifuge Training: The centrifuge is not detailed within the FAA-AST guidelines however it is considered an essential component as part of a training strategy. The benefits of a centrifuge is that it can simulate both Gz profiles (eyeballs down) for the transition between horizontal and vertical flight and Gx profiles (chest to back) for the descent phase. Additionally it is assumed that the SoA pilots will be either test pilots and/or ex-military fast jet pilots who have undergone centrifuge training. However some operators may recruit per the minimum FAA-AST requirements. In either case it will be essential that pilots have centrifuge currency as part of the safety mitigation.
- Simulator Training: The FAA-AST requirements concerning simulator aspects are generally sound and state that the flight crew training device (should) realistically represents the vehicle's configuration and mission. It is imperative that the simulator accurately represents the vehicle in terms of 'concurrency'; this is whereby the configuration is the same as the aircraft (instrumentation, switches, seats, doors, etc.). The rationale is that the other two attributes of a SoA simulator (fidelity and capability) will not accurately reflect the vehicle and therefore can affect the aim of the training. In terms of fidelity (concerning the visual and motion system and accuracy of the instrumentation) it will be extremely difficult to represent high g-forces in all axes. The simulator will not be able to accurately represent the vehicle's capabilities in terms of the 'pull-up', ascent, space segment (with upside down and reaction control aspects) and the high-g descent. Nonetheless, the simulator is an essential component of flight crew training.
- Altitude Chamber Training: Military fast jet pilots (and all other aircrew) are trained to recognize the signs and symptoms of decompression so that they can carry out emergency procedures, including donning an oxygen mask and switching to 100% oxygen under pressure breathing conditions. This is also considered essential for Suborbital flights because the flight crew must be able to respond to the earliest indications of pressurisation problems in order to maintain control of the vehicle. The altitude chamber provides simulated pressurisation failures by climbing the 'chamber' to 25,000 feet (ft), 45,000ft (pressure breathing is required at this altitude).

Strategy 2.1.2 - Argue that FCL Requirements and Guidelines are identified and specific to SoA Operations

The flight crew and passengers are considered an integrated part of the safety of the system; therefore they must be trained and qualified accordingly. In particular to the passengers the following medical qualifications and training requirements apply:

Passenger Medical Qualifications:

It is considered that a minimum standard of fitness and health shall apply to passengers such that they do not become a contributor to a safety event or in the case of a safety event that they are able to undertake the necessary actions.
The passenger medical qualification (PMQ) steps are as follows;

1. Passenger to have medical examination by own General Practitioner (GP) in accordance with a prescriptive format that includes relevant criterion

2. Operator Aerospace Physician to determine suitability of passenger to fly by review of GP certificate of results
3. Operator Aerospace Physician to undertake pre-training medical to determine that the passenger is fit to undertake training in centrifuge and other training as required which may include microgravity flights (Go)
4. Operator Aerospace Physician to undertake pre-flight medical to determine that the passenger is still 'fit to fly' (Go)

EASA are adopting a methodology whereby passengers are either fit to fly (Go), are not fit to fly (No-Go) or have conditions that merit further investigation and risk assessment on an individual basis (Pending Further Checks). An EASA-approved list of contraindicating health issues has been developed as guidelines for operators [Ref TBD].

Passenger Training:

As passengers are considered part of the safety of the system, then the following requirements apply to passenger training:

- Awareness Training/Briefs
- Emergency Training in Simulator (representative hardware);
    - Normal Ingress/Egress
    - Operation of seats and restraining system
    - Emergency Procedures
        - Pressurisation failure
        - Fire
        - Loss of control
        - Crash Landing
        - Emergency egress
        - Medical emergencies
- Centrifuge Training

G2.1.2.1 - Baseline Space Flight Participant Requirements are identified for SoA operations

SFP Medical Requirements

EASA concur with the general requirements for SFPs to undertake a General Practitioner medical with subsequent issue of a certificate. The Operator's aerospace physician (flight surgeon) then determines the suitability of the SFP to undertake the flight. EASA requires that the SFP undergoes a medical by the Operator's aerospace physician immediately prior to centrifuge training and the SoA flight to determine whether the SFP is still fit to fly/train.

SFP Training Requirements

EASA's approach to training is that as safety mitigation, the SFPs are required to undergo essential training that may enable them not to become a flight safety concern during the flight (that may affect the flight crew's ability to maintain control of the flight). Therefore the following are mandated training events:

- Safety Briefings, including emergency briefings
- Centrifuge Training
- Simulator Training, including physical demonstration of normal and emergency situations
- Parabolic Training - only if SFPs are to be allowed to experience microgravity conditions; if SFPs are to remain strapped in during the flight this component of training is not a requirements

G2.1.2.2 - Space Flight Participant Guidelines are effective for SoA operations

SFP Medical Guidelines

EASA concur with the FAA-AST approach to medical requirements but also require that the Operator aerospace physician undertakes a medical on the SFP immediately prior to any centrifuge training or the actual SoA flight

SFP Training Guidelines

- Briefings:

· Space Awareness briefing; this should consist of various videos on the history of human spaceflight, including space tourism, and also provide a tutorial on the space environment and explaining the rationale for some of the training that SFPs will encounter (detailed below)
· SoA briefing; this briefing should be explicitly related to the SoA that the SFPs will fly in. It should include the basic attributes of the vehicles both on the ground and in the air. This should include a video and possibly mock-ups in the classroom environment in order to familiarise the SFPs with the vehicle.
· Emergency briefing; this briefing, once again in the classroom environment, should concern the vehicles safety equipment (fire extinguishers, goggles, oxygen masks, protective clothing) and the actions that SFPs should take in an emergency. SFPs should then be given a 'safety information' booklet that they can study.

- Centrifuge Training: As per flight crew, the centrifuge is not detailed within the FAA-AST guidelines however it is considered an essential component as part of a training strategy. The benefits of a centrifuge is that it can simulate both Gz profiles (eyeballs down) for the transition between horizontal and vertical flight and Gx profiles (chest to back) for the descent phase. In terms of SFPs this is essential because, unlike the pilots/flight crew, they will not have experienced sustained g-forces. They will also not have received Anti-G Straining Manoeuvre (AGSM) training.
- Simulator Training: The simulator is an excellent training tool for the flight crew but in the case of Suborbital flights it can also be an essential part of the SFP training strategy. Having received briefings about the vehicle, the SFPs can then be physically trained on the equipment in terms of the following;

  · Normal Ingress/Egress; it is important that the SFPs are familiar with the basic configuration of the vehicle and are able to enter and exit
  · Operation of Seats; the seats (and restraint system) may actually save their lives so a demonstration and practice in the use of the seat and restrain system is vital. This may be even more important if the seats are designed to recline with certain phases of flight to assist in countering the effects of g-forces.
  · Operation/Procedure for returning to seat (after microgravity phase); should SFPs be allowed to 'float' in the short duration of microgravity then it will be essential that they return to their seat and are restrained for the descent phase. If this does not occur it is envisaged that they will naturally be forced to the floor under the g-forces; this may have dire consequences should another SFP also be forced on top of another SFP as this would result in experiencing twice the weight of the person on the chest resulting in injury or indeed death.
  · Emergency Training
  o Pressurisation failure; depending on the vehicle and operating requirements in the event of a pressurisation failure during the rocket phase and microgravity phase then the vehicle occupants will be in grave danger. This failure condition should then provide a logical argument to provide the occupants with a pressure suit and person oxygen system. The SFPs will then be trained to either shut their helmet or select 100% oxygen (or indeed this may happen automatically). In this instance it is important that SFPs receive full training in the use of their 'spacesuit' and in particular what to do in the event of a pressurisation failure. The author has first-hand experience from the altitude chamber in pressure breathing and it is extremely difficult for 'first-timers' (pilots are used to this).
  o Fire; in the event of a fire whilst airborne there is little the flight crew will be able to do as they will be trying to land the vehicle as quickly and safely as they can. This therefore leads to the issue of fire-fighting. In the event that there is no 'cabin crew' (this would be a good argument to having cabin crew) then it would be up to an SFP to attempt to fight the fire. This leads on to training in the use of the fire-fighting equipment, which could be an issue with some SFPs not being physically or mentally able to do this.

o Loss of control; as occurred on the X-Prize flights, Space-Ship One had an instance of roll 'runaway'. This non-nominal situation could occur on flights and although pilots are trained and used to this sort of manoeuvre, SFPs are certainly not. During the rocket phase and descent phase SFPs should be restrained in their seats and this should not normally be an issue; though it is worth briefing SFPs on and demonstrating the use of a possible 'locked' position of the restraint system.
o Crash Landing; this event could occur from a loss of control incident or other flight events and as per normal aviation a procedure should be implemented and then practiced in the simulator for the SFPs to 'adopt the position' (if appropriate).
o Emergency Egress; in the event of the crashed landing then the SFPs may have to egress quickly. This may involve unstrapping normally or there may be a Quick-Release Button, followed by exiting the vehicle. Once again this can be practiced in the simulator.

In terms of emergency training some operators may feel that demonstrating too many of these aspects may frighten SFPs and so may wish to selectively omit some training. It is considered that the characteristic type of the SFP is an 'adventure seeker' and in fact that they will demand to be involved as much as possible and to undertake as much training as is required. Operators should not reduce safety training as part of cost cutting.

- Parabolic Flight Training: Although not essential for flight crew, should SFPs be allowed to leave their seats in the microgravity phase of the flight then it is considered essential that they have parabolic flight training. The XCOR Lynx vehicle for instance is a two-seater cockpit (one pilot, one fee-paying SFP) and in this instance as the SFP will not be leaving the seat then there is no requirement for parabolic flight training.
- Psychological Training: The physiological training elements detailed above will undoubtedly provide psychological benefits for the SFPs in overcoming any fears or concerns regarding the flight. Indeed much can be done to prepare the SFP for their once-in-a-lifetime experience including a countermeasures program.

  Another psychological benefit of the physiological training is that the SFPs will feel properly integrated with the flight crew and it will no doubt feel for of a team mission rather than a mere individual 'joy-ride'.

Goal 2.2 - Operational Requirements & Guidelines are identified and specific to SoA operations

Goal 3 - EASA SoA ATM/ANS Requirements are effective

Argument 3

Argue that existing ATS/ANS and additional identified SoA requirements are effective to ensure safe SoA operations

Goal 3.1

Existing ATM/ANS Requirements are identified for SoA operators to follow

FAA Applicable Requirements

CFR Part 437.57 - Operating Area Containment
CFR Part 437.69 - Communications
CFR Part 437.71 - Flight Rules
CFR Part 420.31 - Agreements (a. Coastguard, b. ATC)
CFR Part 420.57 - Notifications (NOTAM of flight corridor)

Goal 3.2

Additional ATM/ANS Requirements are identified and specific to SoA operations

Goal 4 - EASA SoA Spaceport Requirements are effective

Argument 4

Argue that the Spaceport Requirements & Guidelines are effective for SoA operations

Goal 4.1

EASA Spaceport Requirements and Guidelines are identified for specific SoA operations

FAA Applicable Requirements

CFR Part 420

Goal 5 - EASA SoA Operator Safety Risk Management Requirements & Guidelines are effective

Argument 5

Argue that Operator Safety Risk Management Requirements & Guidelines are effective for SoA operations

Goal 5.1

Operator Safety Risk Management Requirements are identified and effective for SoA Operators

Goal 5.2

Operator Safety Risk Management Guidelines are effective for SoA operators to follow

FAA Operator Safety Management Guidelines

AC 120-92

ARP 5150

FAA Applicable Guidelines for Spaceports

FAA-AST Environmental Guidelines: these also contain relevant aspects for safety including;

- Airspace
- Hazardous Materials and Hazard Waste Management
- Health and Safety
- Noise

APPENDIX 6 - Exemplar Suborbital Aircraft (Partial) Functional Hazard Analysis – Failure Condition Level

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Systems	Display of attitude information to control roll & pitch	Catastrophic	Catastrophic, if includes both Primary Flight Displays. Major, if includes one pilot's PFD	Catastrophic			Applicable	Applicable
Systems	Display of Heading	Catastrophic Major, if Navigation systems operational	Major	Catastrophic; Major, if Navigation systems operational			Applicable	Applicable
Systems	Display of altitude information	Hazardous	Minor	Catastrophic			Applicable	Applicable
Systems	Display of airspeed information	Hazardous, during landing; otherwise Major	Minor	Hazardous			Applicable	Applicable
Systems	Display of rate of turn	Minor		Minor			Applicable	Applicable
Systems	Display of slip-skid	Minor		Minor			Applicable	Applicable
Systems	Display of time	Minor		Minor			Applicable	Applicable

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Systems	Display of Navigation information	Major; Total Loss of navigation and communication is Catastrophic	Major	Major; Catastrophic for Precision Approaches			Applicable	Applicable
Systems	Communication	Major	Minor	Major, if data is primary link			Applicable	Applicable
Systems	Visibility during landing	Hazardous					Applicable	Applicable
Systems	Misinterpretation of flying altitude	Hazardous		Catastrophic		Occur during landing & poor visibility	Applicable - though SoA may not be certified to CAT I IFR as they may not have an engine and will therefore not be able to 'go-around' in poor visibility landings	Applicable
Systems	Display of Radio Altitude	Minor		Minor		Category I IFR	Not Applicable - though a RAD ALT may be considered as procedural mitigation	Applicable

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Systems	Display of vertical speed	Major		Major		Category I IFR	Although IFR is not applicable, a VSI may be considered essential procedural mitigation	Applicable
Systems	Display of flight guidance commands (Category I operation)	Minor		Minor		Category I ILS For Category II ILS, an autopilot or flight director is required	N/A - SoA may not be certified to CAT I IFR as they may not have an engine and will therefore not be able to 'go-around' in poor visibility landings	Applicable
Systems	Autopilot failure	Hazardous on auto land		Catastrophic if authority is unlimited		Maximum inputs to aircraft primary control surfaces should not exceed aircraft structural limits	N/A	Applicable
Systems	Flight controls for pitch axis	Catastrophic	Major	Catastrophic			Applicable	Applicable

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Systems	Flight controls for roll axis	Hazardous, if yaw axis is still available	Major	Catastrophic			Applicable	Applicable
Systems	Flight controls for yaw axis	Minor to Major. Hazardous to Catastrophic if combined with engine failure or severe cross wind	Minor	Catastrophic			Applicable	Applicable
Systems	Reaction Control System	Hazardous	Hazardous	Catastrophic		Engineering Judgment - additional identified for Suborbital ops	RCS must be able to operate and not interfere with normal controls any stability augmentation system	Not Applicable
Systems	All Hydraulics	Catastrophic					Applicable	Applicable
Systems	Manual control flight controls	Catastrophic					Applicable	Applicable
Systems	Artificial Feel	Hazardous				Variable severity - engineering judgment required	Applicable	Applicable

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Systems	Take-off director and automatic landing system	Catastrophic		Catastrophic, if auto land malfunction below alert height.Hazardous, if take-off director provides only lateral guidance			N/A	if appropriate
Systems	Stability Augmentation	Catastrophic	Catastrophic	Catastrophic		Variable severity - engineering judgment required	if appropriate	Applicable
Systems	Stick Pusher	Hazardous , if stall regime encountered; otherwise Minor	Minor	Hazardous to Catastrophic near ground			if appropriate	Applicable
Systems	Flaps for take-off/ landing	Hazardous for landing		Hazardous to Catastrophic if asymmetric		Engineering judgment	if appropriate	Applicable

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Systems	Stick shakers/stall warning	Minor	Minor	Major		Assumes that a warning system is in place to notify pilot of loss of system function	if appropriate	Applicable
Systems	Trim control	Minor	Minor	Major, if manual trim. Catastrophic or hazardous for electrical			if appropriate	Applicable
Systems	Display of trim indicators	Minor	Minor	Major; engineering judgment		Variable severity - engineering judgment required	if appropriate	Applicable
Systems	Landing Gear control	Hazardous	Minor	Major to Hazardous			Applicable	Applicable
Systems	Display of landing gear indications	Major		Hazardous			Applicable	Applicable

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Systems	Brake control	Catastrophic, if unannunciated loss of braking. Major if annunciated loss of braking	Hazardous	Hazardous		Electronic anti-skid and brake systems can cause significant ground handling problems if they malfunction under adverse conditions due to asymmetrical loading	Applicable	Applicable
Systems	Visual warnings, cautions and alerts	Major for worst case				Failure conditions depend on the criticality of the systems being monitored and pilot action required	Applicable	Applicable
Systems	Display of outside air temperature	Minor	R	Minor		R = Reserved	if appropriate	Applicable

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Systems	Display of toxic gas levels	Catastrophic	Catastrophic	Catastrophic		Engineering Judgment - additional identified for Suborbital ops	closed loop system so need to ensure levels of CO2 are not high and incapacitate pilots	N/A
Systems	Over speed warning	Minor	Minor	Minor		Airspeed may be used as a backup to the over speed warning for continued safe flight and landing	May need to up the severity to Major?	Applicable
Systems	Aural warnings					Failure conditions depend on the criticality of the systems	Applicable	Applicable
Systems	Warning of fire in cabin	Hazardous				Engineering Judgment - additional identified for Suborbital ops	Applicable	Applicable

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Systems	Ventilation/internal fan blower system	Hazardous				Engineering Judgment - additional identified for Suborbital ops	Applicable	N/A
Systems	Electrical system indication	Minor	Minor	Major		Depends on crew reference and analysis	Applicable	Applicable
Systems	Vacuum/pressure indication	Minor	Minor	Major		Provides an indication that flight instruments are operating within power source limits	if appropriate	if appropriate
Systems	Electrical Power	Catastrophic, if primary flight instruments require electrical power	Hazardous for IFR. Depends on capability of secondary system	Installation dependent		Depends on electrical system loads (from analysis) and the criticality of the functions	Catastrophic due to critical systems	Applicable
Power plant	Uncontained disk failure				Catastrophic		N/A (see note 5)	Applicable
Power plant	Engine/Pylon separations				Catastrophic		N/A (see note 5)	Applicable
Power plant	Engine/rocket case rupture				Catastrophic		Applicable	Applicable

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Power plant	Uncontained blade failures				Hazardous	Uncontained fan blade failures, or uncontained turbine blade failures or uncontained compressor blade failures	N/A (see note 5)	Applicable
Power plant	Core cowl separations				Catastrophic		N/A (see note 5)	Applicable
Power plant	Inlet Cowl separations				Catastrophic		N/A (see note 5)	Applicable
Power plant	Fan cowl separations				Hazardous		N/A (see note 5)	Applicable
Power plant	Nozzle separations				Hazardous		Applicable	Applicable
Power plant	Liberation of large nacelle/fairing parts				Hazardous		Applicable	Applicable
Power plant	Liberation of small nacelle/fairing parts				Major		Applicable	Applicable
Power plant (Thermal)	Fire damage outside designated fire zones				Catastrophic		Applicable	Applicable

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Power plant (Thermal)	Fire damage within designated fire zones				Hazardous		Applicable	Applicable
Power plant (Thermal)	Magnesium fires				Hazardous	Variable - engineering judgment required	if appropriate	if appropriate
Power plant(Thermal)	Electrical fires				Hazardous to Catastrophic	Variable - engineering judgment required	Applicable	Applicable
Power plant (Thermal)	Loss of power plant installation thermal insulation				Hazardous to Catastrophic	Variable - engineering judgment required	Applicable	Applicable
Power plant (Thermal)	Inadvertent release of engine (or APU) bleed air				Hazardous to Catastrophic	Variable - engineering judgment required	N/A (see note 5)	
Power plant (Thermal)	Inadvertent engine (or APU) exhaust gas impingement				Hazardous to Catastrophic	Variable - engineering judgment required	N/A (see note 5)	

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Power plant (Excess Loads)	Excessive engine/rocket (or APU) vibration				Variable - engineering judgment required; Hazardous?		Applicable -Exposure of 90 sec for calculation	Applicable
Power plant (Excess Loads)	Explosive ignition of flammable vapours				Catastrophic		Applicable -Exposure of 90 sec for calculation	Applicable
Power plant (Excess Loads)	Rupture of pressurised components (oxidiser tank)				Hazardous		Catastrophic for SoA	Applicable
Power plant (Excess Loads)	Inadvertent firing of rocket				Catastrophic	Engineering Judgment - additional identified for Suborbital ops	Applicable	N/A
Power plant (Excess Loads)	Engine (or APU) seizure loads				Hazardous		N/A (see note 5)	Applicable

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Power plant(Excess Loads)	Abnormal thrust vectors				Variable - engineering judgment required; Hazardous?	Causes by engine mount failures, inadvertent thrust reverser deployment, compressor surge, nozzle failures, etc.	Nozzle blockage/ asymmetric ablation	Applicable
Power plant (Excess Loads)	Fuel Imbalance				Variable - engineering judgment required; Hazardous?	Caused by asymmetric loading or use of fuel, or leaking or trapped fuel, or improper transfer	N/A (see note 5)	Applicable
Power plant (thrust)	Thrust Loss (detected) 2 to 55% (twins)				Minor to Hazardous (note 2)	Take off abort/ over-run from take-off power set to V1	N/A (see note 5)	Applicable
Power plant (thrust)	Thrust Loss (detected) 2 to 55% (twins)				Minor to Major (note 3)	Air turn back/diversion after V1	N/A (see note 5)	Applicable
Power plant (thrust)	Thrust Loss (undetected) 2 to 55% (twins)				Minor to Catastrophic (note 4)	Unable to clear obstacle during any flight phase	N/A (see note 5)	Applicable

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Power plant (thrust)	Thrust Loss (detected) > 55% (twins)				Minor to Hazardous (note 2)	Take off abort/ over-run from take-off power set to V1	N/A (see note 5)	Applicable
Power plant (thrust)	Thrust Loss (undetected) > 55% (twins)				Catastrophic	Over-run/unable to clear obstacle from take-off power	N/A (see note 5)	Applicable
Power plant (thrust)	Thrust Loss > 55% (twins)				Catastrophic	Unable to maintain altitude during take-off between V1 and 1500' AGL	N/A (see note 5)	Applicable
Power plant(thrust)	Thrust Loss > 55% (twins)				Catastrophic	Unable to maintain altitude during en-route	N/A (see note 5)	Applicable
Power plant (thrust)	Rocket Thrust Loss				Major to Hazardous	Engineering Judgment - additional identified for Suborbital ops;	In this instance, the SoA would abort the rocket phase and recover stability and then do a normal glide/approach	N/A

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Power plant (thrust)	Inadvertent in-flight thrust reversal				Hazardous to Catastrophic		N/A (see note 5)	Applicable
Power plant (thrust)	Loss of reverse thrust				Minor to Catastrophic	During landing or rejected take-off (severity dependent on runway condition)	N/A (see note 5)	Applicable
Power plant (thrust)	Loss of thrust control required to meet certification or operational control manoeuvrability, or crew workload requirements				Major to Catastrophic		Possibly due to loss of fluids through zero-g (so must have mitigation of fluid systems designed to cope with zero-g)	**Applicable only if carrier is to perform parabolic flights:** Possibly due to loss of fluids through zero-g (so must have mitigation of fluid systems designed to cope with zero-g)

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Power plant(thrust)	Loss of system redundancy or functionality due to engine (or APU) failure				Variable - engineering judgment required; Hazardous?	Caused by loss of electrical power generation, or hydraulics pumps, or ECS bleed air, or anti-ice bleed air	N/A (see note 5)	Applicable
Power plant (display)	Display of fuel level indication	Minor	Minor	Major			fluid systems must cope with zero-g phase	Applicable only if carrier is to perform parabolic flights: fluid systems must cope with zero-g phase
Power plant (display)	Display of power plant oil temperature	Minor	Minor	Minor			N/A (see note 5)	Applicable
Power plant (display)	Display of power plant oil pressure	Minor	Minor	Minor			N/A (see note 5)	Applicable only if carrier is to perform parabolic flights: fluid systems must cope with zero-g phase

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Power plant (display)	Display of hydraulic pressure	Hazardous for SS2, Minor for WK2	Hazardous for SS2, Minor for WK2	Hazardous for SS2, Minor for WK2		Engineering Judgment - additional identified for Suborbital ops	fluid systems must cope with zero-g phase	Applicable only if carrier is to perform parabolic flights: fluid systems must cope with zero-g phase
Power plant (display)	Display of power plant fuel pressure	Minor	Minor	Major			Applicable	Applicable
Power plant (display)	Display of rocket fuel pressure	?	?	?		Variable - engineering judgment required; Hazardous?	Applicable	N/A
Power plant(display)	Display of power plant/rocket thrust	Major	Minor	Hazardous			Applicable	Applicable
Power plant (display)	Display of power plant/rocket fire warning	Major	Major	Hazardous			Applicable	Applicable
Power plant (display)	Display of power plant thrust reverser position	Major		Major			N/A (see note 5)	

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Propellant	Fuel or propellant/ oxidiser feed/fuel supply				Major to Hazardous (depending on phase) for SS2; Catastrophic FOR WK2		Applicable	Applicable only if carrier is to perform parabolic flights: fluid systems must cope with zero-g phase
Propellant	Rocket abort				Catastrophic	Engineering Judgment - additional identified for Suborbital ops	should a non-nominal situation occur (LOC or excessive vibration) then the rocket phase must be able to be aborted to avoid a Catastrophic outcome	N/A
Propellant	fuel/propellant/ oxidiser tank integrity				Catastrophic		Applicable	Applicable
Propellant	fuel/propellant/ oxidiser jettison				Hazardous		could be Catastrophic	could be Catastrophic

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Propellant	Un-commanded fuel/propellant/ oxidiser jettison				Hazardous to Catastrophic		Applicable	Applicable
Ice Protection	Inlet, engine or other power plant ice protection on multiple power plants when required				Hazardous		N/A (see note 5)	Applicable
Ice Protection	engine/power plant ice protection				Hazardous		N/A (see note 5)	Applicable
Ice Protection	Activation of engine inlet ice protection above limit temperatures				Hazardous		N/A (see note 5)	Applicable
Pressurisation	Cabin Decompression				Hazardous to Catastrophic		Applicable	Applicable
Structure	Control surfaces structural failure				Hazardous to Catastrophic		Applicable	Applicable

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Structure	Landing gear structural failure on hard landing or soft ground				Catastrophic		Applicable	Applicable
Structure	Loss of vent and pressurization (fuel/oxidizer system)				Catastrophic		Applicable	Applicable
Fire Risks	Fire risk due to oxygen				Catastrophic		Fire suppression system needs to be considered for closed loop cabin	Applicable
Fire Risks	Fire risk due to electrical faults in equipment				Catastrophic	bonding, such that effects of lightning are minimized	Fire suppression system needs to be considered for closed loop cabin	Applicable
Fire Risks	Fire risk due to overheating brakes				Catastrophic		Dependant on individual SoA design	Applicable
Other Risks	Wheels up landing				Hazardous		Applicable	Applicable

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
Other Risks	Loss of cabin egress capability				Hazardous to Catastrophic		Applicable	Applicable
Other Risks	Unintended Spaceship - Carrier separation				Hazardous if sufficient height to obtain aerodynamic glide to land; otherwise Catastrophic		Engineering judgment as new technology	Hazardous or No effect?
Other Risks	Loss of (airframe) ice protection when required				Hazardous		N/A	As required
Other Risks	Seat Restraint whilst under 'g' force				Hazardous	Engineering Judgment - additional identified for Suborbital ops	Marginal to Hazardous to participants	Applicable only if carrier is to perform parabolic flights: Marginal to Hazardous to participants

References:	This FHA list has been compiled from example FHA in AC23.1309, ARP 5150 and the EASA paper (Marciacq et.al) and knowledge of existing functions for spaceflight operations with a Carrier/Spaceship configuration
Notes:	

		Classification of Failure Condition				Comment		
Systems	Function	Total Loss of Function (with warning)	Loss of Primary Means of Providing Function	Misleading and/or Malfunction (without warning)	General Functional Failure (Loss or Incorrect)		Comments and Applicability to **Suborbital Aircraft**	Comments and additional applicability to **Carrier aircraft (for the SoA)**
	Note 1: % is total aircraft/spaceship thrust. Threshold values are based on typical (aircraft only) margins. Thrust reductions caused strictly by pilot error are not considered a 'Thrust Loss Scenario' for the purpose of this table. The failure condition severities noted here are based solely on the effects of thrust loss and not on any other potential effects of causal failures (e.g. potential hazards associated with damage from an uncontained engine failure, loss of electrical or hydraulic systems are not reflected here). therefore these severities are generally dependent on the effects of the thrust loss scenario has on aircraft performance relative to certified field length or obstacle clearance limits (i.e. see 14 CFR Part 121 Subpart I and 14 CFR Part 25 Subpart B).							
	Note 2: The worst case scenario is where the thrust is such that it occurs throughout the take-off roll but is only detected at or near V1 and the aircraft is too far down the runway to avoid a high speed over-run.							
	Note 3: The severity of the effects from these performance losses will be dependent on the aircraft type design, the mission, and the scenario.							
	Note 4: The two scenarios here which produce the greatest risk of striking an obstacle, either during take-off or en-route, are; a) operating for an extended period of time with a small symmetric thrust loss (2 to 15%) followed by an engine failure; and b) operating for a short period (perhaps a flight or two) with a larger thrust loss.							
	Note 5: For Suborbital Aircraft (SoA) the engine-related failures have been noted as 'Not Applicable' (N/A/) as it is assumed that the SoA do not have engines for normal flight i.e. only a rocket. However it is appreciated that some designs may incorporate a rocket and an engine(s) - in this case, the engine-related functions and failures thereof are applicable.							

APPENDIX 7 - Exemplar Suborbital Aircraft (Partial) Functional Hazard Analysis – Aircraft Level

The following exemplar aircraft level FHA is provided to illustrate the functional failure conditions and the derived aircraft level Key (Platform) Hazard. Only the first few functions are shown to illustrate the technique (Block 1.1 to 2.2):

Aircraft Function	FBD Ref	Specific Function	Functional Failure Guide Word	Functional Failure	Effect	Classification	Resultant Failure Condition	Resultant platform level Key (Platform) Hazard
1.1 PROVIDE THRUST	1.1.1	PROVIDE ENGINE MOTIVE SOURCE	Omission	No thrust provided when required	As per normal aviation	Catastrophic	Loss of Engine Thrust	Undetected inappropriate Engine Thrust
			Commission	Thrust provided when not required	As per normal aviation	Hazardous	Un-commanded Engine Thrust	
			Incorrect	Thrust incorrect	As per normal aviation	Hazardous	Incorrect (PARTIAL) Engine Thrust	
	1.1.2	PROVIDE ROCKET MOTIVE SOURCE	Omission	No/Loss of Rocket thrust when required	Flight Aborted - glide to land or power up aero-engines	Major-Hazardous	Loss of Rocket Thrust	Undetected inappropriate Rocket Thrust
			Commission	Rocket Thrust provided when not required	If connected to a carrier aircraft could be catastrophic - if not, then would be hazardous to catastrophic depending on flight phase	Catastrophic - Hazardous	Un-commanded Rocket Thrust	
			Incorrect	Asymmetric thrust vector	Incorrect thrust vector resulting in Non-nominal flight path	Catastrophic	Incorrect (PARTIAL) Rocket Motive Force	
1.2 PROVIDE CONTROL OF	1.2.1	PROVIDE GROUND STABILITY	Omission	Loss of stability on the ground		Hazardous	Loss of stability on the ground	Undetected inappropriate

AIRCRAFT ON GROUND			Commission	Ground Stability provided when not required		Hazardous	N/A	Ground Stability
			Incorrect	Incorrect stability		Hazardous	N/A	
	1.2.2	PROVIDE BRAKING	Omission	No braking when required on ground		Hazardous	Loss of braking	Undetected inappropriate Braking
			Commission	Braking when not required on ground		Hazardous	Un-commanded braking	
			Incorrect	Incorrect braking		Hazardous	Incorrect braking	
	1.2.3	PROVIDE STEERING	Omission	Loss of steering when required		Hazardous	Loss of steering	Undetected inappropriate Steering
			Commission	Steering input when not required		Hazardous	N/A	
			Incorrect	Incorrect Steering		Hazardous	Incorrect Steering	
1.3 PROVIDE CONTROL OF AIRCRAFT ATTITUDE	1.3.1	PROVIDE CONTROL OF AIRCRAFT PITCH ATTITUDE	Omission	Loss of ability to control pitch attitude		Hazardous-Catastrophic	Loss of pitch attitude control	Undetected inappropriate Flight Control
			Commission	Un-commanded change in pitch attitude		Hazardous-Catastrophic	Un-commanded change in pitch attitude	
			Incorrect	Incorrect pitch attitude/incorrect speed control		Hazardous-Catastrophic	Incorrect pitch control	
	1.3.2	PROVIDE CONTROL OF AIRCRAFT ROLL ATTITUDE	Omission	Loss of ability to control aircraft roll attitude		Hazardous-Catastrophic	Loss of roll attitude control	Undetected inappropriate Flight Control
			Commission	Un-commanded change in aircraft roll attitude		Hazardous-Catastrophic	Un-commanded change in roll attitude	
			Incorrect	Incorrect roll attitude/incorrect heading		Hazardous-Catastrophic	Incorrect roll control	

	1.3.3	PROVIDE CONTROL OF AIRCRAFT YAW ATTITUDE	Omission	Loss of ability to control aircraft yaw		Hazardous-Catastrophic	Loss of yaw attitude control	Undetected inappropriate Flight Control
			Commission	Un-commanded change in aircraft yaw		Hazardous-Catastrophic	Un-commanded change in yaw attitude	
			Incorrect	Incorrect yaw attitude		Hazardous-Catastrophic	Incorrect Yaw attitude	
	1.3.3	PROVIDE STABILITY AUGMENTATION (SPACE SEGEMENT)	Omission	Loss of ability to stabilize ac	SoA may not be in optimum angle for descent and may lose control	Hazardous-Catastrophic	Loss of Reaction Control System	Undetected inappropriate Stability Augmentation (or same as above i.e. undetected inappropriate flight control)
			Commission	Un-commanded stability augmentation	May change flight path but should have little effect	N/A	N/A	
			Incorrect	Incorrect stability augmentation	N/A - Subset of above	N/A	N/A	
1.4 PROVIDE STRUCTURAL INTEGRITY	1.4.1	PROVIDE PRIMARY STRUCTURAL INTEGRITY	Omission	Loss of aircraft primary structural integrity		Catastrophic	Loss of aircraft primary structural integrity	Undetected inappropriate Structural Failure
			Commission	Provision of primary structural integrity when not required	N/A	N/A	N/A	
			Incorrect	Incorrect primary structural integrity	N/A	N/A	N/A	
	1.4.2	PROVIDE SECONDARY STRUCTURAL INTEGRITY	Omission	Loss of aircraft secondary structural integrity		Hazardous	Detachment of secondary structure	Undetected inappropriate Structural Failure
			Commission	Provision of secondary structural integrity when not required	N/A	N/A	N/A	
			Incorrect	Incorrect secondary structural integrity	N/A	N/A	N/A	

	1.4.3	PROVIDE DYNAMIC ELEMENTS INTEGRITY	Omission	Loss of aircraft dynamic integrity	control surfaces structural failure may lead to loss of control/loss of structural integrity	Hazardous-Catastrophic	Loss of aircraft dynamic structural integrity	Undetected inappropriate Structural Failure
			Commission	Provision of dynamic integrity when not required	N/A	N/A	N/A	
			Incorrect	Incorrect dynamic integrity	N/A	N/A	N/A	
1.5 PROVIDE VISIBILITY	1.5.1	PROVIDE VISIBILITY OF OUTSIDE WORLD	Omission	Loss of visibility of the outside world		Hazardous	Loss of external visibility from the aircraft.	Undetected inappropriate SoA Position
			Commission	Visibility of the outside world when not required	N/A	N/A	N/A	
			Incorrect	Incorrect external visibility	N/A	N/A	N/A	
	1.5.2	PROVIDE VISIBILITY OF AIRCRAFT INTERIOR	Omission	Loss of visibility of aircraft interior		Hazardous	Loss of visibility of the aircraft interior	Undetected inappropriate SoA Position
			Commission	Visibility of the aircraft interior when not required	N/A	N/A	N/A	
			Incorrect	Incorrect internal visibility	N/A	N/A	N/A	
2.1 PROVIDE OPERATIONAL AWARENESS OF AIRCRAFT STATE	2.1.1	PROVIDE DISPLAY OF ALTITUDE	Omission	Loss of ability to provide barometric display		Minor		Undetected inappropriate Altitude
			Commission	Un-commanded barometric display	N/A	N/A	N/A	

			Incorrect	Incorrect barometric display		Hazardous		
	2.1.2	PROVIDE DISPLAY OF ATTITUDE	Omission	Loss of ability to provide attitude display		Catastrophic		Undetected inappropriate Attitude
			Commission	Un-commanded attitude display	N/A	N/A	N/A	
			Incorrect	Incorrect attitude display		Catastrophic		
	2.1.3	PROVIDE DISPLAY OF SPEED	Omission	Loss of ability to provide airspeed display		Major-Hazardous		Undetected inappropriate Speed
			Commission	Un-commanded airspeed display	N/A	N/A	N/A	
			Incorrect	Incorrect airspeed display		Hazardous		
	2.1.6	PROVIDE DISPLAY OF HEADING	Omission	Loss of ability to display aircraft heading		Major-Hazardous		Undetected inappropriate Heading
			Commission	Un-commanded change in aircraft displayed heading		N/A	N/A	
			Incorrect	Incorrect display of aircraft heading		Hazardous		
2.2 PROVIDE AIRCRAFT CURRENT POSITION AND NAVIGATION DATA	2.2.1	PROVIDE CURRENT AIRCRAFT POSITION	Omission	Loss of current aircraft position		Major-Hazardous		Undetected inappropriate SoA Position
			Commission	Position determined when not required		N/A	N/A	
			Incorrect	Incorrect position determined		Hazardous	Undetected incorrect aircraft position error.	
	2.2.2	PROVIDE AIRCRAFT FLIGHT PATH GUIDANCE	Omission	Loss of ability to provide aircraft flight path guidance		Hazardous	N/A	Undetected inappropriate Flight Path
			Commission	Relative position of destination determined when not required	N/A	N/A	N/A	

			Incorrect	Incorrect Flight Path		Catastrophic for Precision approaches - otherwise Hazardous	Undetected incorrect aircraft flight path selection.	
		Guide Words	Omission	Means failure to operate, lack of indication or warning, jammed or free operation				
			Commission	Means inadvertent or uncommanded operation, and false indication or warning				
			Incorrect	Means intermittent operation, partial or degraded operation, nuisance indications or warnings, false or delayed data input/output or display. Runaway (full or partial), changes in characteristics				
		Key (Platform) Hazards	Key (Platform) Hazards derived from the FHA are highlighted in the final column as detailed here:					Denotes a Key (Platform) Hazard (platform level)
		Lower-Level System Hazards (Failure Conditions)	Those Functional Failures derived from the FHA that are highlighted in the second to last column are considered relevant but are lower-level functional failures i.e. system-level failure conditions				Denotes a lower system-level failure condition	

APPENDIX 8 - PAPER 1 – Operators SMS; presented at IAC, Valencia, 2006

SUBMISSION FOR 57th IAF Category E3.4

SAFETY MANAGEMENT OF SPACE TOURISM

Charles Andrew Quinn MSc AMRAeS – High Wycombe, UK

ABSTRACT

Travelling at 3 times the speed of sound during the ascent and experiencing 5 times Earth's nominal gravitational forces during re-entry is not a normal flight profile. How does the general public, let alone highly trained flight crew, cope with these and other exacting environmental factors during a suborbital spaceflight? To enable the innovative space tourism industry to achieve success, designers and operators must constantly view the challenge from a safety perspective. The Federal Aviation Administration (FAA) has produced regulatory guidelines to cover the varying design proposals of prospective Re-Launch Vehicle (RLV) operators and these guidelines provide baseline measures. The challenge for the RLV operators is to employ criteria to meet and exceed the guidelines.

This paper examines the challenges using a Safety Management System (SMS) approach. The author has undertaken the available training for the space participants to gather experiential research data, including radial G-Force experience (centrifuge and flight in an RAF Hawk), simulated zero-G forces (parabola flight), aircraft simulator training, disorientation training (disorientation motion simulator and 3-axis 'spaceball'), and hyperbaric training (decompression chamber and pressure breathing). This practical data, together with the theoretical analysis of American and Russian operated space flight profiles, and the Scaled Composite's SpaceShipOne profile, enabled the author to identify key issues that need to be addressed; G-Forces, Life Support Systems, Noise, Vibration, Radiation and Medical standards. A high-level Safety Case methodology was reviewed, employing the Goal Structured Notation (GSN) model, whereby evidence was examined to support arguments that the overall goal is satisfied – 'the flight crew and space participants are acceptably safe for spaceflight'.

The findings verified the requirement for an SMS approach, including safety by design in the early stages being a critical factor. The practical research phase highlighted that psychological and physiological management of the flight crew, especially for the space participants, is vital to assure

the success of the industry. The outcome of the research included recommendations for an SMS approach, including mitigating measures in order to satisfy and exceed FAA requirements. It is concluded that exacting environments require high levels of safety management, both in design and operation; an RLV with in-built safety features still requires an effective safety culture embedded within an operator's effective SMS to avoid a disastrous event. Space tourism can be successful, so long as safety management principles are proactively employed from the beginning and with commitment at all levels of the industry.

Full paper at:

www.saturnsms.com

APPENDIX 9 - PAPER 2 – Micro-Gravity; Presented To QinetiQ for UK CAA Consideration

CERTIFICATION CONSIDERATIONS FOR MICRO-GRAVITY FLIGHTS WITHIN UK

C.A. Quinn – QinetiQ, Bristol, UK

Abstract

The emergence of the Commercial Spaceflight Industry has provided opportunities for companies in regards of design, manufacture, operations and training. Within the latter field, parabolic flights to facilitate 'micro-gravity' experiences are regarded as integral to a spaceflight Operator's passenger training programme. Currently, there are no UK CAA regulations covering this activity. To enable micro-gravity flights to commence within the UK, regulations and guidance need to be produced in advance to permit the activity.

This paper examines differing approaches to micro-gravity flight certification and the necessary methodology to ensure the safe management of the activity. The paper also presents the view that micro-gravity flights should be granted permission to fly, qualifying under the CAA's Certificate of Airworthiness by demonstration of compliance within defined modification and verification standards.

Full paper at:

www.saturnsms.com

APPENDIX 10 - PAPER 3 – Centrifuge as Key Safety Mitigation; presented at IAASS, Rome, Italy, October 2008

Submitted for: The IAA 1st Symposium on Private Manned Access to Space

Commission III (Space Technology and System Development)

CENTRIFUGE TRAINING AS KEY SAFETY MITIGATION IN THE COMMERCIAL SPACEFLIGHT INDUSTRY

Authors

Andy Quinn MSc AMRAeS IEng	-	Operations Director, Worldview Spaceflight
Dr Henry Lupa	-	Senior Physiologist, QinetiQ
Alec Stevens	-	Physiologist, QinetiQ

Abstract

Sub-orbital spaceflight profiles may nominally incur gravitational forces up to 4Gz and/or 4Gx during the ascent, depending on spacecraft design, and up to 7Gx during the descent, once again depending on spacecraft design and also procedures. Will the general public cope with these extreme stresses on the body, especially considering that the duress may exceed 90 seconds during ascent and then again during descent? The emergence of the commercial spaceflight industry has provided opportunities for companies in regards of design, manufacture, operations and training. Within the latter field, centrifuge training to facilitate gravitational forces should be regarded as key to a spaceflight operator's passenger training programme. Currently, there are no regulatory requirements for

passengers to undertake centrifuge training, with the Federal Aviation Administration (FAA) stating that passengers should have ‘emergency briefs’.

This paper examines the role of centrifuge training as part of an effective safety management system (SMS), including a comprehensive training programme for passengers (and indeed flight crew) as part of risk mitigation. The justification for centrifuge training will be quantified by numerical evidence from centrifuge runs carried out on non-military and non-astronaut candidates in practical runs involving video footage and the measurement of vital statistics. The paper also presents the view that an effective aerospace medical pre-screening process should also be considered essential as part of the mitigation process. Effective safety management would mitigate extreme gravitational forces to as low as reasonably practical by introducing design features, warnings, training, processes and procedures.

The findings of the paper verified the rationale for the centrifuge training, combined with an effective aerospace medical pre-screening process in assuring the safety of passengers for sub-orbital spaceflight. Assessment of each individual’s g-tolerance was considered essential and the subsequent training and techniques were found to be invaluable in the prevention of g-induced loss of consciousness (G-LOC). It is concluded that prospective spaceflight passengers should participate in centrifuge training in order to provide both physiological and psychological mitigation against the extreme environment. It is therefore recommended that Regulators of the emerging commercial spaceflight industry introduce centrifuge training as a pre-requisite element of Space Operator’s preparation of their passengers.

Full paper at:

www.saturnsms.com

APPENDIX 11 - PAPER 4 – Safety Criteria for the Personal Spaceflight Industry; presented at IAASS, Huntsville, USA, May 2010

Submitted for: The Fourth IAASS Conference – Making Safety Matter
Session – 'Private Spaceflight Safety'

SAFETY CRITERIA FOR THE PRIVATE SPACEFLIGHT INDUSTRY

Authors
Andy Quinn MSc AMRAeS IEng - Saturn Safety Management Systems Ltd
Professor Paul Maropoulos CEng FCIRP FIMechE - University of Bath, England

Abstract

The sub-orbital private spaceflight industry, whilst still in its developmental stages, remains one of the most the eagerly anticipated and closely watched new industries of the past few years. The Federal Aviation Administration (FAA) has set specific rules and generic guidelines to cover experimental and operational flights by industry forerunners such as Virgin Galactic and XCOR. One such guideline [Advisory Circular 437.55-1, dated April 20, 2007] contains 'exemplar' hazard analyses for spacecraft designers and operators to follow under an experimental permit; in particular stating that the guidelines are *not mandatory* and that they are *for demonstrating compliance with certain requirements associated with the launch or re-entry of a reusable suborbital rocket.* However in terms of severity classifications, the hazard analysis guideline merely considers harm to the public and the public property. The guideline stops short of providing meaningful guidance on the safety criteria and on determining the loss of the spacecraft (cumulative probability of safety critical failures). The Advisory Circular does not attempt to address the potential differences in risk levels with the different launch design solutions, such as vertical launches, horizontal single stage launches and airborne launches. This issue is also considered in a report to the United States Congress entitled '*Analysis of Human Space Flight Safety*' where the authors (members of The Aerospace Corporation, George Washington University and the Massachusetts Institute of Technology) cite that the industry is too immature and has *insufficient data* to be proscriptive and that '*defining a minimum set of criteria for human spaceflight service providers is potentially problematic'* in order not to '*stifle the emerging industry'*. The authors of this paper contend that it is better practice to have a sound safety engineering approach that can be modified with time as opposed to redrawing unsound criteria when accidents occur. This paper aims to address the problematic issue of safety criteria for the emerging personal spaceflight industry. Our methodology is firstly to synthesise 'best practice' approaches from the aviation and space industries. These will in turn provide the basis for a set of proposals and guidelines which will provide more robust safety criteria than those currently defined in FAA guidelines. We also examine the current hazard analysis Advisory Circular 437.55-1 and argue that additional clarification is needed to assist and inform spacecraft designers, constructors and operators. These groups should have been/should be using these guidelines now to construct their own System Safety Program Plans to be able to *'demonstrate compliance with certain requirements'* for experimental permits; the authors acknowledge the immaturity of the industry yet contend that these groups should be assisted and not left to define their own criteria. The paper also argues for more clarity in definitions and intent for using the classification tables as criteria in the current guidelines.

Full paper at: www.saturnsms.com

APPENDIX 12 - PAPER 5 – An Integrated Safety Model for Suborbital Spaceflight, presented at IAASS, Paris, France, Oct 2011

Submitted for: The Fifth IAASS Conference – Making Safety Matter
Session – 'Commercial Human Spaceflight Safety'

NEW SAFETY MODEL FOR THE COMMERCIAL HUMAN SPACEFLIGHT INDUSTRY

Authors

Andy Quinn MSc MRAeS CEng - Saturn Safety Management Systems Ltd

Dr Steve Bond PhD MRAeS CEng - City University, London, England

Professor Paul Maropoulos - University of Bath, England

Abstract

The aviation and space domains have safety guidelines and recommended practices for Design Organisations (DOs) and Operators alike. In terms of Aerospace DOs there are certification criteria to meet and to demonstrate compliance there are Advisory Circulars or Acceptable Means of Compliance to follow. Additionally there are guidelines such as Aerospace Recommended Practices (ARP), Military Standards (MIL-STD 882 series) and System Safety Handbooks to follow in order to identify and manage failure conditions. In terms of Operators there are FAA guidelines and a useful ARP that details many tools and techniques in understanding Operator Safety Risks. However there is currently no methodology for linking the DO and Operator safety efforts. In the space domain NASA have provided safety standards and guidelines to follow and also within Europe there are European Co-operation of Space Standardization (ECSS) to follow. Within the emerging Commercial Human Spaceflight Industry, the FAA's Office of Commercial Space Transportation has provided hazard analysis guidelines. However all of these space domain safety documents are based on the existing aerospace methodology and once again, there is no link between the DO and Operator's safety effort.

This paper addresses the problematic issue and presents a coherent methodology of joining up the System Safety effort of the DOs to the Operator Safety Risk Management such that a 'Total System' approach is adopted. Part of the rationale is that the correct mitigation (control) can be applied within the correct place in the accident sequence. Also this contiguous approach ensures that the Operator is fully aware of the safety risks (at the accident level) and therefore has an appreciation of the Total System Risk.

The authors of this paper contend that it is better practice to have a fully integrated safety model as opposed to disparate requirements or guidelines. Our methodology is firstly to review 'best practice' approaches from the aviation and space industries, and then to integrate these approaches into a contiguous safety model for the commercial human spaceflight industry.

Full paper at:

www.saturnsms.com

APPENDIX 13 - Safety Suborbital Space Safety Technical Committee 'Explanatory Note'

The Author proposed to have a new Technical Committee (TC) for Suborbital Space Safety (SSS) because of the uniqueness of the new field; the current Space Safety & Launch Safety Committees were mainly concerned with Orbital (Governmental) Safety and would not necessarily understand the need for a new approach for the (nominally) aircraft-based Suborbital vehicles. The 'Explanatory Note' contains the author's views and ideas on how the new SSS TC could be formed and how the TC could influence safety in the suborbital domain.

PURPOSE

The purpose of this new Suborbital Space Safety Technical Committee (SSS TC) is to focus on the emerging technical issues as the industry develops towards regular suborbital operations. The timing for introducing this TC is pertinent with the leading companies entering their flight test phases; thus the media will be and the world will be watching to determine for themselves the viability and safeness of this exciting new venture.
The SSS TC will address technical issues for suborbital operations only and will cover the following all modes of operation:

- Horizontal take-off (with either powered or un-powered approach and landing) – typically a EADS (Atrium) model
- Horizontal Rocket Launch (with either powered or un-powered approach and landing) – typically an XCOR model
- Air Launch (with either powered or un-powered approach and landing) – typically a Virgin Galactic model
- Vertical Rocket Launch and Recovery – typically a Blue Origin model
- Plus any other emerging mode of operation in the suborbital domain

The rationale for a separate TC is that some of the above modes of operation have aircraft-based designs and therefore may adhere to standard aviation recognised practices and certification approaches. Additionally as the suborbital flight profile has a more contained 'footprint' the emphasis for safety must primarily include the airworthiness/ space-worthiness of the vehicle in order to protect those on board as well as those in support of the take-off or launch and of course, the general public (3rd parties);the effect to 3rd parties should be minimised in the case of suborbital flights because the NOTAM area will be in a sparsely populated area (as opposed to an Orbital launch or re-entry whose trajectory will overly populated areas at some point).

INTEGRATION WITH EXISTING TECHNICAL COMMITTEES

Whilst the SSS TC will focus on the suborbital technical issues there may be an overlap of safety topics concerning other TCs. Where a topic is clearly more suited to another TC, then that TC should either have already addressed the issue or the new issue should be raised by the SSS TC with the relevant TC to deal with. Once the issue has been discussed in the TC the outcome shall be reviewed and further discussed within the SSS TC to achieve consensus.
The following issues of overlap are anticipated:

- Suborbital Vertical Launches only; interaction required of the Launch Safety TC
- Suborbital Human Factors and Performance issues; interaction required with the HFPS TC
- Suborbital 'Space' segment of flight; interaction required with the Legal Regulatory Committee

MEMBERS

The members for the SSS TC is composed of relevant Agency personnel and IAASS General Members; both of these categories of people have been chosen for their knowledge, interest and professional attributes such that a credible body can be constituted to provide informed judgement on suborbital space safety matters.

Committee Role	Name and Organisation	Contact Details
Chair	Andy Quinn (Saturn SMS)	Andy.quinn@iaass.org
Co-Chair	Maite Trujillo (ESA)	Maite.trujillo@iaass.org
Agency Member	Jean-Bruno Marciacq (EASA)	Jean-Bruno.Marciacq@easa.europa.eu
Agency Member	Melchor Antunano (FAA)	Melchor.J.Antunano@faa.gov
Space Society Member	Norul Ridzuan (Malaysian STS)	ikam290200@hotmail.com
Industry Member	Christophe Chavagnac (EADS-Astrium)	christophe.chavagnac@astrium.eads.net
Industry Member	Chuck Lauer – Rocketplane (Spacelinq)	ChuckLauer@aol.com
General Members	Diane Howard (McGill University – Air & Space Law)	ladydi814@me.com
General Members	Tanya Masson-Zwaan (Deputy Director International Institute of Air & Space Law)	t.l.masson@law.leidenuniv.nl
General Members	Simon Adebola – previous IAASS paper on Emergency Medicine for Human Suborbital Spaceflight	simonadebola@gmail.com
General Members	Amaya Atencia Yepez (GMV) – Systems RAMS expert and has also worked in the aerospace domain	aatencia@gmv.com
Other Specialists Invited	Dr Eric Groen (TNO) – expert in aerospace medical and human factors specialist	eric.groen@tno.nl
Other Specialists Invited	Manual Vals Toimil (previous ESA head of integration crew missions)	mvallstoimil@gmail.com
Other Specialists Invited	Arno Wilders – Space Horizon	arno@spacehorizon.com
Other Specialists Invited	Misuzo Onuki	mszmail@aol.com
Other Specialists Invited	Karin Nilsdotter	karin@spaceportsweden.com
Other Specialists Invited	Rafael Harillo Gomez-Pastrana	harillo@stardust-consulting.es

SUBORBITAL TOPICAL ISSUES

The SSS TC will address issues only relating to suborbital space safety

(a) General – Papers/Workshops/Panels

- Current Status and Development of Suborbital Industry – Paper (relevant for presentation to:
  - UNCOPUOS (June 2011)
  - 5th IAASS Suborbital Space Safety Panel Discussion (Oct 2011)
- 2-day workshop to support IAASS Conference? (on technical issues below)
- ISSF-IAASS workshop (on technical issues below)
- Preside over Suborbital Space Safety Panel Discussion and Sessions at the IAASS Conferences
- Technical Issues
  - Defining & Harmonization of Safety Criteria
  - Defining & Harmonization of Certification ‘v’ Launch Licensing
  - Provide Guidance on Design System Safety Analysis for Suborbital vehicles
  - ECLSS

  - Rockets
  - Propellants
  - Other suborbital specific design issues
- Provide Guidance on Suborbital Operations:
  - Operator Safety Risk Management for Suborbital vehicles
  - Pilot Considerations (qualifications and training)
  - Passenger Considerations (medical and training)
  - Spaceport Considerations
  - ATM Considerations
- Promotion of Sector
  - Newsletter
  - Attending Relevant Conferences
  - Publications
- Update to IAASS – ISSB Space Safety Standard Manual (Commercial Human-Rated System)
- Monitoring of Occurrences/Advice to Accident Investigations